17.4.2 Access point centric Test Profiles

Access point centric test profile means that all individual active tests are run against an access point at once. After all active tests of the profile are run against the access point, the profile proceeds to test against the next access point. Access point centric profile can be configured so that all active tests are run within a single association with the access point. This helps reducing workload of authentication servers.

If the test profile introduced in the previous chapter would be access point centric, the execution order of the tests would be the following:

Table 9: Test execution order on access point centric test profile

Attach AP1 **Ping AP1** Detach AP1	⇨	Attach AP1 **TCP download AP1** Detach AP1	⇨	Attach AP1 **TCP upload AP1** Detach AP1	⇨	Attach AP2 **Ping AP2** Detach AP2
Attach AP2 **TCP download AP2** Detach AP2	⇨	Attach AP2 **TCP upload AP2** Detach AP2	⇨	Attach AP3 **Ping AP3** Detach AP3	⇨	Attach AP3 **TCP Download AP3** Detach AP3
Attach AP3 **TCP upload AP3** Detach AP3	⇨	**Managed scan**	⇨	Attach AP1 **Ping AP1** Detach AP1	⇨	Attach AP1 **MOS uplink AP1** Detach AP1
Attach AP1 **MOS downlink AP1** Detach AP1	⇨	Attach AP2 **Ping AP2** Detach AP2	⇨	Attach AP2 **MOS uplink AP2** Detach AP2	⇨	Attach AP2 **MOS downlink AP2** Detach AP2
Attach AP3 **Ping AP3** Detach AP3	⇨	Attach AP3 **MOS uplink AP3** Detach AP3	⇨	Attach AP3 **MOS downlink AP3** Detach AP3	⇨	**Noise monitor**

As it can be seen, now the execution order of the tests differs from the execution order of test centric profile. All active tests are run in a row for each access point.

If the profile is configured to remain associated between tests, the monitoring station does not detach from the access point after a test but remains associated until the test profile proceeds to a next access point or a passive test.

Table 10: Test execution order on access point centric test profile, remain associated

Attach AP1			Attach AP2
Ping AP1	TCP download AP1	TCP upload AP1	Ping AP2
		Detach AP1	
		Attach AP3	
TCP download AP2	TCP upload AP2	Ping AP3	TCP Download AP3
	Detach AP2		
	Managed scan	Attach AP1	
TCP upload AP3		Ping AP1	MOS uplink AP1
Detach AP3			
	Attach AP2		
MOS downlink AP1	Ping AP2	MOS uplink AP2	MOS downlink AP2
Detach AP1			Detach AP2
Attach AP3			Noise monitor
Ping AP3	MOS uplink AP3	MOS downlink AP3	
		Detach AP3	

17.5 Operations on templates

Templates are for copying and editing. There are two different supported methods for that, “Duplicate” to make a fresh copy of the sample profile and “Copy as essid” that adds the template profile to an existing test profile.

17.5.1 Duplicate

1. Select “Manage | Test Profiles” to open the management tree on the left.
2. Choose the appropriate template and right-click for the submenu.
3. Select “Duplicate” to open the Test Profile pane.
4. Give a name to the new Test Profile.
5. Bound Tests window is for informative purposes here only. Editing if desired is available later.
6. Select “Execution mode”. Access point centric execution mode also allows the monitoring station to remain associated between (active) tests.
7. In “Common Values” one may enter test parameters that apply to every test in the profile.
8. Saving options
    a. Select “Cancel Changes” to undo changes.
    b. Select “Keep Changes to save the intermediate work.
    c. Select “Save All Changes” to finalize the work on this pane.

17.5.2 Copy as essid

The pre-requisite here is to have existing test profiles that shall be the target for pasting all elements in the template. This is one form of cut&paste operation.

1. Select “Manage | Test Profiles” to open the management tree on the left
2. Choose the appropriate template and right-click for the submenu
3. Select “Copy as essid” (no visible results)
4. Right-click on Test Profile icon and select “Insert essid” to open essid pane on the right
5. Insert an existing essid name
6. Optionally, insert other common parameters in the table “Common Values”
7. Select “Save All Changes” to insert the test elements in the template to the test profile as individual essid. All tests under the essid contain the same parameters, such as Sonar etc.

17.6 Operation on Test Element

17.6.1 Copy element

The pre-requisite here is to have existing test profiles that shall be the target for pasting this test element. This is one form of cut&paste operation.

1. Select “Manage | Test Profiles” to open the management tree on the left
2. Choose one of the test elements and right-click
3. Select “Copy element” (no visible results)
4. Paste the element by choosing “Paste testprofile element” available on the right-click
    a. If the target is a Test Profile icon, the element shall be the last one in that profile
    b. If the target is an essid inside a test profile, the element shall be the last one for that essid.
5. Repeat step 2-4 until the test profile is according the expectations.

17.6.2 Configure Ethernet test

An active test can be configured to be run via Ethernet interface of the monitoring station. This can be configured on Test Element level:

1. Select “Manage | Test Profiles” to open the management tree on the left
2. Choose one of the test elements and right-click
3. Select “Edit”
4. In the dialog, change “WLAN” to “Ethernet” on NetworkInterfaceType row.
5. Select “Save All Changes”

17.7 Operations on Test Profile Node

Save All Changes

Any change in the sub-tree shall be made persistent.

Add empty Test Profile

A new test profile object to the tree shall be inserted. The only input required is the name of the profile and the execution mode.

17.8 Operations on Test Profile

Edit

Open a pane with “Common Values” and “Name” field ready for editing. “Bound Tests” remains read-only, the elements are managed in the tree.

Duplicate

Create identical test profile with a new name. It is possible to change top-level parameters on the same pane. This option enables easy creation of test profiles with similar test elements to another link.

Copy as essid

Copies the contents of a test profile to be pasted to another profile as essid object.

Remove

Removes the object.

Bound Eyes

Shows the monitoring stations that are using this profile.

Paste test profile element

Paste previously copied test profile element as the last element in the profile.

Save

Make the changes in the sub-objects persistent.

Insert Essid

Paste previously copied essid into this profile as the last element.

Insert New Essid

Create a new empty essid into this profile as the last element.

Export

Export test profile content in text file.

17.9 Operations on essid inside a test profile

Edit

Open a pane with "Common Values" and "Name" field ready for editing.

Copy

Enable pasting of the object.

Paste test profile element

Paste previously copied test profile element as the last element in the profile.

Remove

Deletes the object.

17.10 On test elements

Each test has default parameters, which can be used as is or modified as needed. To obtain the best results and find the best measurement methods for a target network, plan and configure the tests to suit the network.

A test profile must be configured for each monitoring station separately. The same profile can be used in several monitoring stations.

17.10.1 Modifying test parameter and test name

If you wish to modify individual tests, see the instructions below. For each test, do the following:

1. Select the test from the profile and right-click the test
2. Select "Edit"
3. If desired, change test name (for example, for distinguishing Ethernet tests)
4. If desired, set the test duration (in seconds)
    a. The test duration does not affect the running of the test; however, if the test type is temporarily removed from the test set, the time specified is spent in sleep mode, depending on the configuration
5. For some tests you may also do the following:
    a. Select the interval, or the pause between pings
    b. Select Sonar
    c. Select SIP server (if SIP register test is configured)
    d. Select an access point
    e. Select an IP address (non DHCP only)
    f. Select a net mask (non DHCP only)
    g. Select a default gateway (non DHCP only)
    h. Select the number of bytes to be downloaded/uploaded
    i. Select the number of repetitions
    j. Select the client's IP address policy:
        i. DHCP in use (1)
        ii. Static address (0) – enter address data
    k. Select network interface type: WLAN or Ethernet

6. Select “Keep changes”
7. Select “Save all changes”

17.10.2 Disabling and enabling test elements

A test element within test profile can be disabled. This means that the test is excluded from the test profile and the test won’t be run until it is enabled again. Disabled and enabled test profile elements can be identified by their colors (see beginning of the chapter 17).

How to disable a test element:

1. Select the test element from the profile and right-click
2. Select “Disable element”

How to enable a test element:

1. Select the test element from the profile and right-click
2. Select “Enable element”

17.10.3 Use case: Multiple SSID testing

There are two ways to achieve testing on multiple networks on one single monitoring station. The first is based on element copying (the previous paragraph) and the other is using copies of essid objects.

Using copies of elements may be burdensome at the configuration time but gives control over the test order. By copying one single element (test type) to be sequentially tested on different WLANs produces the following sample profile:

1. TCP on Wlan1
2. TCP on Wlan2
3. TCP on Wlan3
4. Spectrum
5. MOS on Wlan1
6. MOS on Wlan2
7. MOS on Wlan3
8. Scan

The other approach is the create a simple test sequence as essid and then duplicate the essid object and make the duplicates to point to different WLANs. The resulting sample test profile would be similar to the following:

1. TCP on Wlan1
2. MOS on Wlan1
3. Spectrum
4. TCP on Wlan2
5. MOS on Wlan2
6. Scan
7. TCP on Wlan3
8. MOS on Wlan3

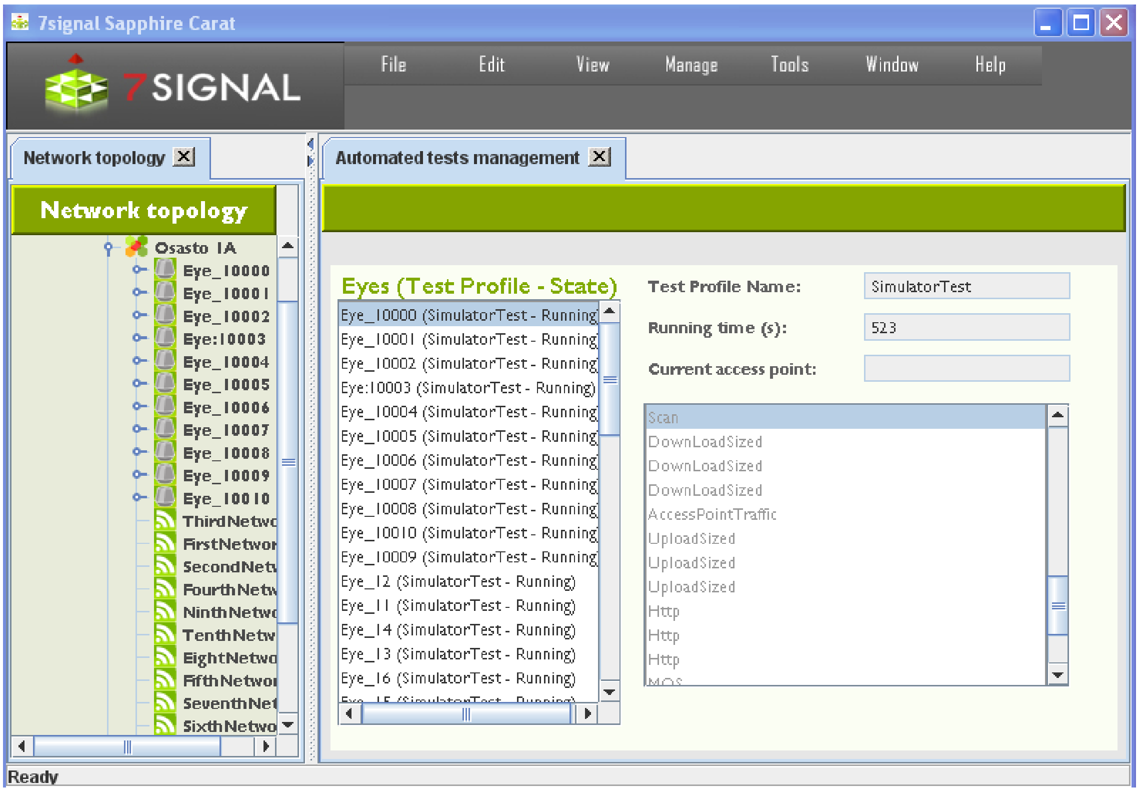
Please observe that in the latter approach the measurements on a single WLAN network shall be sparser temporally. While individual tests shall happen on roughly the same time interval, the distribution of the samples per network differs a great deal on these two approaches.

When planning the test cycles, one should bear in mind:

- The more tests there are in the sequence, the bigger the difference in sample distribution.
- The more networks, the fewer samples for individual networks.

17.11 Running Test Profiles

Select “Tools | Automated tests management” to see current status of Eye units.



Eyes (Test Profile - State)

Eye_10000 (SimulatorTest - Running
Eye_10001 (SimulatorTest - Running
Eye_10002 (SimulatorTest - Running
Eye:10003 (SimulatorTest - Running)
Eye_10004 (SimulatorTest - Running
Eye_10005 (SimulatorTest - Running
Eye_10006 (SimulatorTest - Running
Eye_10007 (SimulatorTest - Running
Eye_10008 (SimulatorTest - Running
Eye_10010 (SimulatorTest - Running
Eye_10009 (SimulatorTest - Running
Eye_12 (SimulatorTest - Running)
Eye_11 (SimulatorTest - Running)
Eye_14 (SimulatorTest - Running)
Eye_13 (SimulatorTest - Running)
Eye_16 (SimulatorTest - Running)
Eye_15 (SimulatorTest - Running)

Test Profile Name: SimulatorTest
Running time (s): 523
Current access point:

Scan
DownLoadSized
DownLoadSized
DownLoadSized
AccessPointTraffic
UploadSized
UploadSized
UploadSized
Http
Http
Http
MOS

Figure 35: Automated tests management view

The Eyes of the user context are enlisted in the box on the right. The Eye name, the test profile name and the state of the test profile run are indicated.

By selecting one of the Eyes brings additional information such as the run time and test profile content on the left.

17.12 Automated tests and KPIs

Each automated test produces measurement data for one or more KPIs. The following table represents which automated test produces data for which KPI.

Table 11: Test profile elements and KPIs

Test profile element	KPIs
Surveillance	CL001
Network Scan	AV001 AV004 AV009-AV011 QURS004 QURS010
Managed AP scan	AV001 AV008 AV009 QURS002 QURS003 QURS010
Ping	AC001 AC002 AC004-AC014 AV002 QUAP032 QURT004 QURT007
Http	AC001 AC002 AC004-AC014 AV002 QUAP007 QUAP028 QUAP031 QUAP032 QUFR070-QUFR081 QUFR118-QUFR129 QUIP013
SIPRegister	QUAP040-QUAP045 RE020-RE022
TCP upload TCP download	AC001 AC002 AC004-AC014 AV002 QUAP001 QUAP002 QUAP011 QUAP012 QUAP016 QUAP019 QUAP032 QUAP037

	QUFR034- QUFR069 QUFR118-QUFR129 QUIP005 QUIP006 QURS026-QURS032 RE001 RE002 RE004
VoIP MOS	AC001 AC002 AC004-AC014 AV002 QUAP005 QUAP006 QUAP013 QUAP015 QUAP022 QUAP025 QUAP032-QUAP036 QUFR082-QUFR129 RE005 RE011 RE012
Noise monitor	QURS001
Access point traffic	QURS004-QURS008 TR001-TR003 TR012-TR015 TR018-TR023
Spectrum analysis	SP001-SP004
Air utilization	TR030-TR040 TR138
Access point radio environment	TR050-TR060
Access point traffic + collect frame details option	TR100-TR137 TR140-TR145 TR200- TR331 TR400-TR473 TR500-TR573 TR600-TR673 TR700-TR709

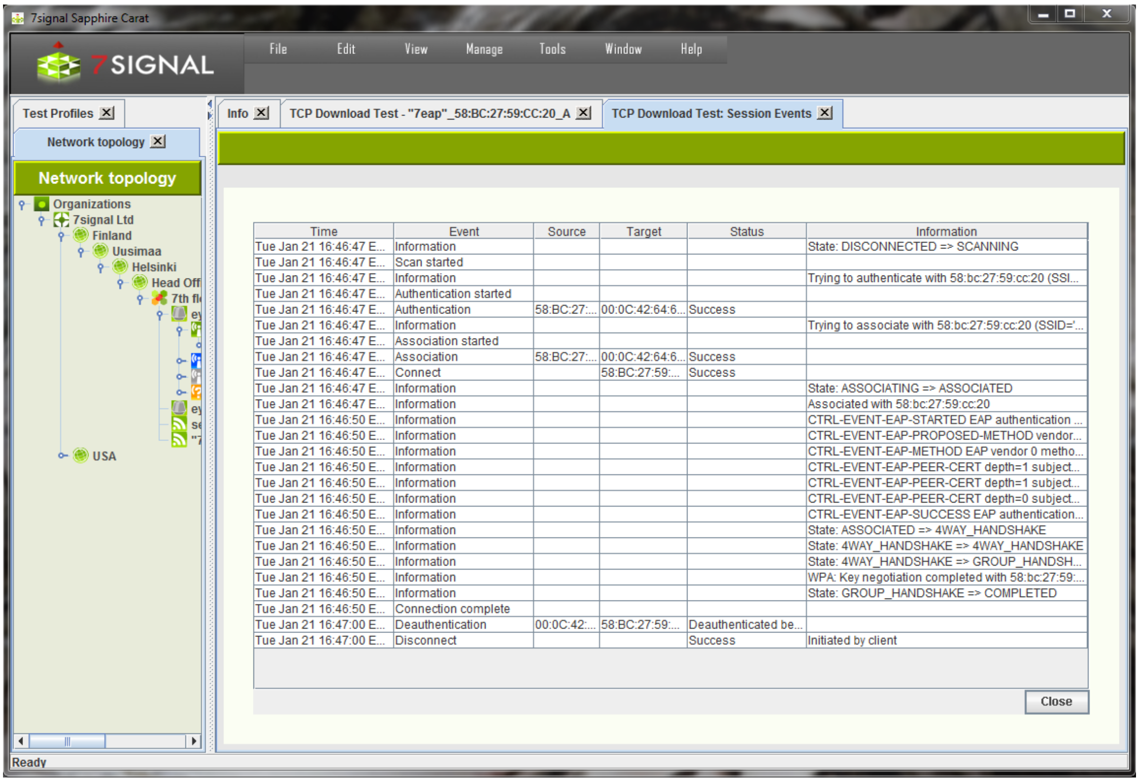
18 MANUAL TESTS

Manual tests can run simultaneously with automated testing. Sapphire will perform ongoing automated test first and then run user defined manual test. Automated test will continue after manual test has been finished.

Manual test results will not be saved to database.

18.1 Session events

Session events can be shown from active tests (i.e. tests in which the monitoring station associates with an access point). If the test supports session events, the test dialog contains “Session events” button.



Time	Event	Source	Target	Status	Information
Tue Jan 21 16:46:47 E...	Information				State: DISCONNECTED => SCANNING
Tue Jan 21 16:46:47 E...	Scan started				
Tue Jan 21 16:46:47 E...	Information				Trying to authenticate with 58:bc:27:59:cc:20 (SSI...
Tue Jan 21 16:46:47 E...	Authentication started				
Tue Jan 21 16:46:47 E...	Authentication	58:BC:27:...	00:0C:42:64:6...	Success	
Tue Jan 21 16:46:47 E...	Information				Trying to associate with 58:bc:27:59:cc:20 (SSID='...
Tue Jan 21 16:46:47 E...	Association started				
Tue Jan 21 16:46:47 E...	Association	58:BC:27:...	00:0C:42:64:6...	Success	
Tue Jan 21 16:46:47 E...	Connect		58:BC:27:59:...	Success	
Tue Jan 21 16:46:47 E...	Information				State: ASSOCIATING => ASSOCIATED
Tue Jan 21 16:46:47 E...	Information				Associated with 58:bc:27:59:cc:20
Tue Jan 21 16:46:50 E...	Information				CTRL-EVENT-EAP-STARTED EAP authentication ...
Tue Jan 21 16:46:50 E...	Information				CTRL-EVENT-EAP-PROPOSED-METHOD vendor...
Tue Jan 21 16:46:50 E...	Information				CTRL-EVENT-EAP-METHOD EAP vendor 0 metho...
Tue Jan 21 16:46:50 E...	Information				CTRL-EVENT-EAP-PEER-CERT depth=1 subject...
Tue Jan 21 16:46:50 E...	Information				CTRL-EVENT-EAP-PEER-CERT depth=1 subject...
Tue Jan 21 16:46:50 E...	Information				CTRL-EVENT-EAP-PEER-CERT depth=0 subject...
Tue Jan 21 16:46:50 E...	Information				CTRL-EVENT-EAP-SUCCESS EAP authentication...
Tue Jan 21 16:46:50 E...	Information				State: ASSOCIATED => 4WAY_HANDSHAKE
Tue Jan 21 16:46:50 E...	Information				State: 4WAY_HANDSHAKE => 4WAY_HANDSHAKE
Tue Jan 21 16:46:50 E...	Information				State: 4WAY_HANDSHAKE => GROUP_HANDSH...
Tue Jan 21 16:46:50 E...	Information				WPA: Key negotiation completed with 58:bc:27:59:...
Tue Jan 21 16:46:50 E...	Information				State: GROUP_HANDSHAKE => COMPLETED
Tue Jan 21 16:46:50 E...	Connection complete				
Tue Jan 21 16:47:00 E...	Deauthentication	00:0C:42:...	58:BC:27:59:...	Deauthenticated be...	
Tue Jan 21 16:47:00 E...	Disconnect			Success	Initiated by client

Figure 36: Session events

Session events describe time line and state of the radio link. Typical session event list can be seen in the figure above. The columns of the session event table are the following:

- **Time:** When the action resulted the event occurred
- **Event:** Type of the event. Possible actions resulting a session event are the following:
    - **Scan started:** The monitoring station has started to scan an access point
    - **Authentication started:** The monitoring station has started to authenticate itself to an access point
    - **Authentication:** The monitoring station has authenticated itself to an access point
    - **Association started:** The monitoring station has started to associate with the access point.
    - **Association:** The monitoring station has associated with the access point
    - **Connect:** Radio link is ready
    - **Connection complete:** Radio link and authentication are complete

- **Deauthentication:** Monitoring station has deauthenticated itself from the access point
- **Disconnect:** Monitoring station has disconnected itself from the access point
- **Information:** Various types of information events
  - **State:** State change
  - **CTRL-EVENT-***: Internal supplicant events related to e.g. EAP authentication.

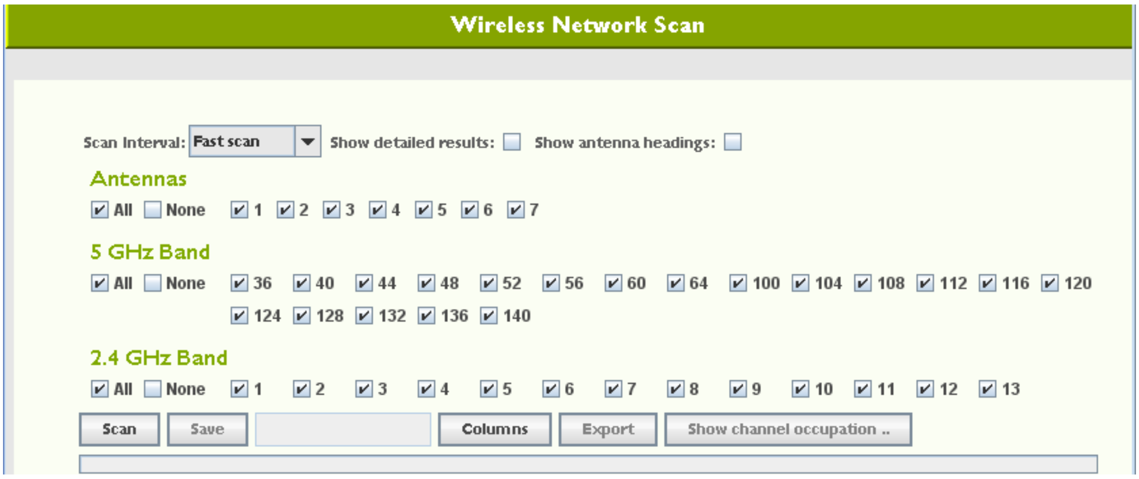
- **Source:** Source MAC address causing the event. Either the MAC address of the monitoring station or the access point.
- **Target:** Destination MAC address causing the event. Either the MAC address of the monitoring station or the access point.
- **Status:** Status of the operation. Status or reason code defined by the 802.11 standard.

18.2 Network scan test

The network scan test can also be used as a separate test outside initial deployment. The deployment is described in the previous section of this guide.

To scan the network, do the following:

1. In the Network topology, select the Eye you want to use for scanning the network
2. Right-click and select “Network Scan”; a test window is displayed in the right pane
3. Select the test duration from the pull-down menu
4. If you want to view information about each antenna, select “Show detailed results”
   a. If this checkbox is selected, the results window has a separate line for each antenna, which might make the window’s content more difficult to read
5. If you want to see compass heading from which the access point was heard, select “Show antenna headings”[15]
6. Select the scan directions – i.e., directional antennas[15]
7. Select the channels to scan
8. Select “Scan”
9. The results are displayed in a table



Wireless Network Scan

Scan Interval: Fast scan ▾ Show detailed results: □ Show antenna headings: □

Antennas

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7

5 GHz Band

☑ All □ None ☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52 ☑ 56 ☑ 60 ☑ 64 ☑ 100 ☑ 104 ☑ 108 ☑ 112 ☑ 116 ☑ 120 ☑ 124 ☑ 128 ☑ 132 ☑ 136 ☑ 140

2.4 GHz Band

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13

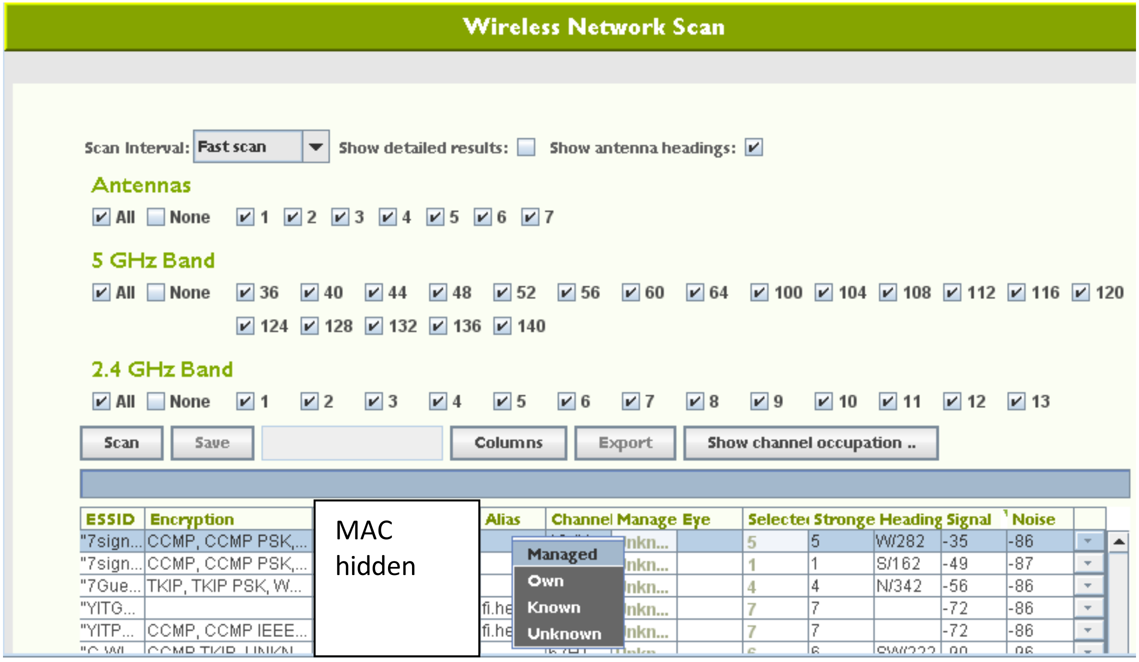
Figure 37: Wireless network scan test

[15] Antenna selection is not possible in Soft and Micro Eyes. Only one antenna is available.

After the network scan, you can verify the suitability of the selected antenna by running the antenna selection test.

The information in the table can be edited. Remember to save the changes.

- “Manage”: The management status: the managing status of a monitoring station against this access point can be changed
- “Selected Ant”: Selected antenna – you can change the antenna used by the Eye to monitor the access point[16]
    - We recommend that you compare the signal levels received very thoroughly
    - We recommend that you perform the antenna selection test if anything is even slightly unclear



Wireless Network Scan

Scan Interval: Fast scan ▾ Show detailed results: □ Show antenna headings: ☑

Antennas

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7

5 GHz Band

☑ All □ None ☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52 ☑ 56 ☑ 60 ☑ 64 ☑ 100 ☑ 104 ☑ 108 ☑ 112 ☑ 116 ☑ 120 ☑ 124 ☑ 128 ☑ 132 ☑ 136 ☑ 140

2.4 GHz Band

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13

ESSID	Encryption	Alias	Channel	Manage	Eye	Selecte	Stronge	Heading	Signal	Noise
"7sign...	CCMP, CCMP PSK,...			Unkn...		5	5	W/282	-35	-86
"7sign...	CCMP, CCMP PSK,...			Unkn...		1	1	S/162	-49	-87
"7Gue...	TKIP, TKIP PSK, W...			Unkn...		4	4	N/342	-56	-86
"YITG...		fi.he		Unkn...		7	7		-72	-86
"YITP...	CCMP, CCMP IEEE...	fi.he		Unkn...		7	7		-72	-86

Figure 38: Selecting managing role for an access point

Options for processing the results:

- “Save” saves the information in the table to the Carat system.
- “Columns” select the visible columns; the table might be easier to read if you hide unnecessary columns
- “Export” exports a text file to the local file system – you can enter the location in the dialog that appears after you click “Export” – which is a handy feature for comparison of results obtained at different times

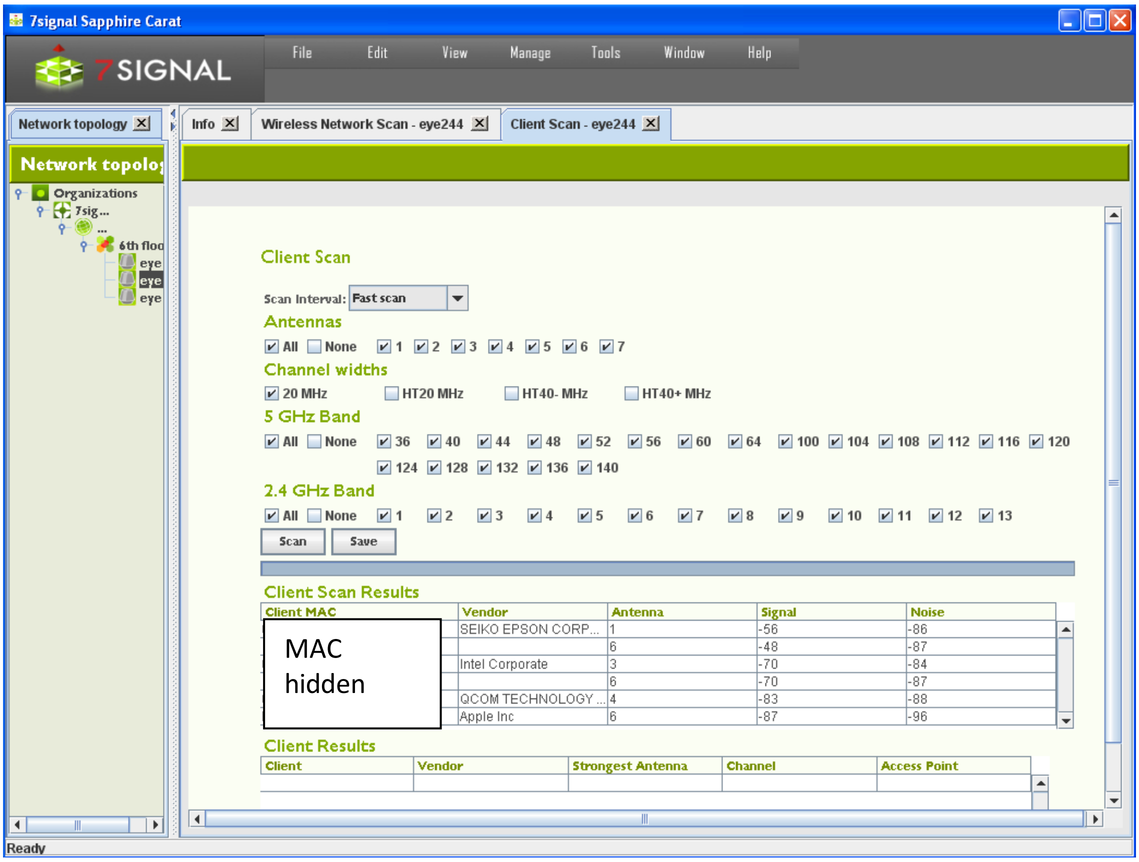
18.3 Client scan test

You can scan for preconfigured clients by their MAC address.

1. In the Network topology, select the Eye you want to use for scanning the network
2. Right-click and select “Active Tests | Client Scan”
3. Enter the scan duration under “Scan interval”
4. Select the scan directions – i.e., antenna lobes[16]

[16] Only one antenna can be selected in Soft and Micro Eyes

5. Select channel widths
6. Select the channels to scan
7. Select “Scan”
8. The results are displayed in a table:
    a. The MAC address of the scanned devices that transmitted during the test
    b. The noise level and signal strength, by antenna



Client Scan

Scan Interval: Fast scan

Antennas

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7

Channel widths

☑ 20 MHz □ HT20 MHz □ HT40- MHz □ HT40+ MHz

5 GHz Band

☑ All □ None ☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52 ☑ 56 ☑ 60 ☑ 64 ☑ 100 ☑ 104 ☑ 108 ☑ 112 ☑ 116 ☑ 120 ☑ 124 ☑ 128 ☑ 132 ☑ 136 ☑ 140

2.4 GHz Band

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13

Client Scan Results

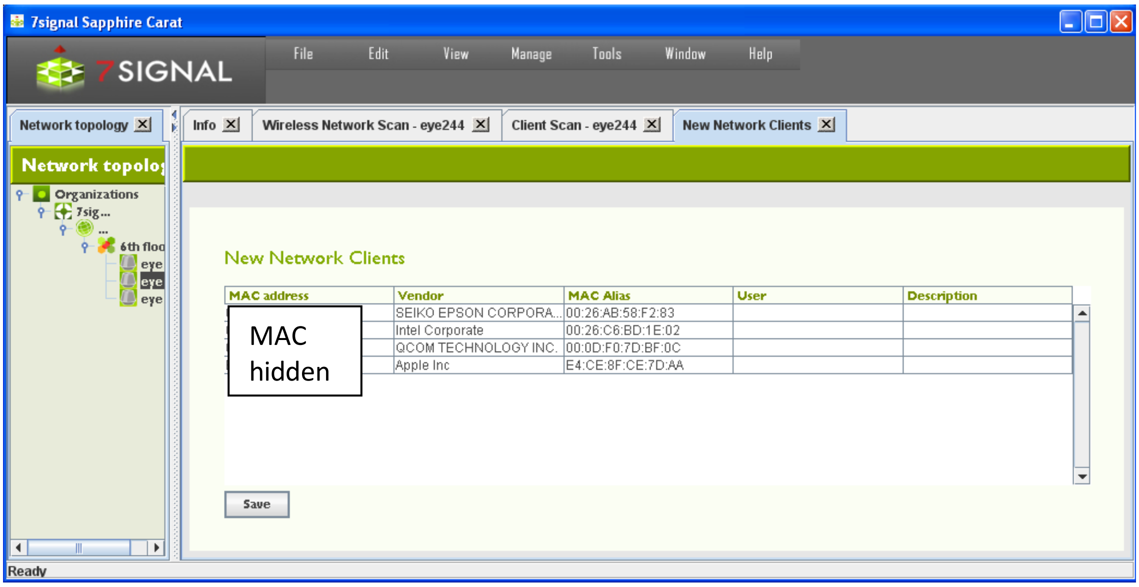
Client MAC	Vendor	Antenna	Signal	Noise
MAC hidden	SEIKO EPSON CORP...	1	-56	-86
		6	-48	-87
	Intel Corporate	3	-70	-84
		6	-70	-87
	QCOM TECHNOLOGY ...	4	-83	-88
	Apple Inc	6	-87	-96

Client Results

Client	Vendor	Strongest Antenna	Channel	Access Point

Figure 39: Client scan results

9. Select “Save”; the clients detected remain in the table
10. You can enter a friendly name and description for each user; this name will be displayed in future results instead of the MAC address



New Network Clients

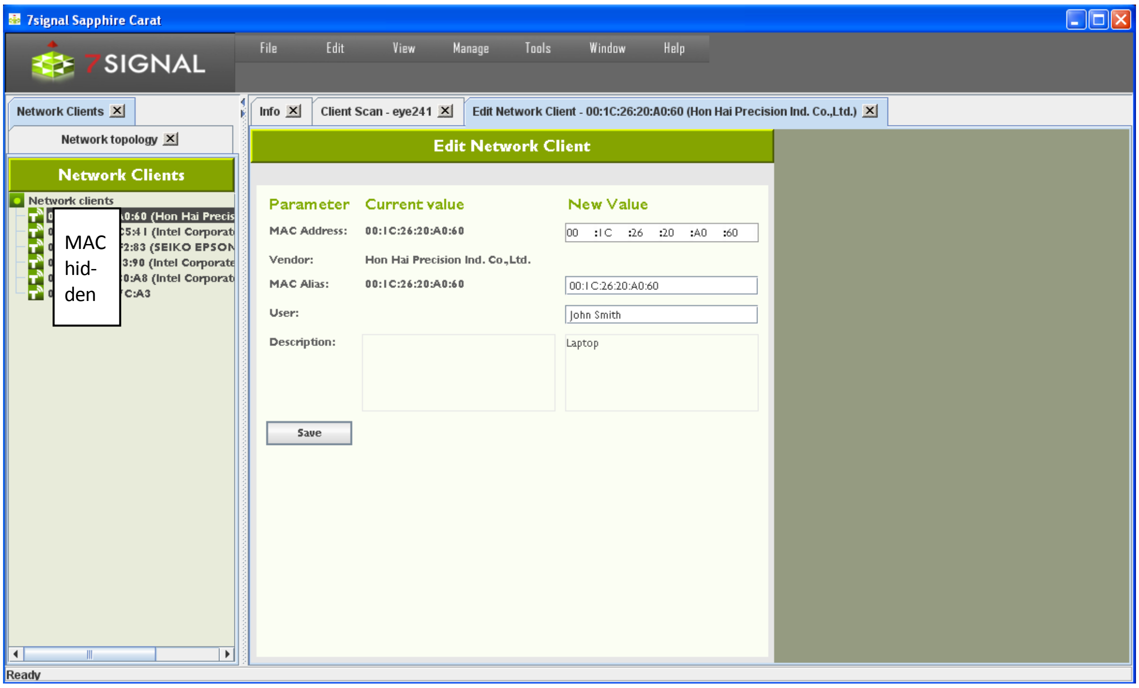
MAC address	Vendor	MAC Alias	User	Description
	SEIKO EPSON CORPORA...	00:26:AB:58:F2:83		
	Intel Corporate	00:26:C6:BD:1E:02		
	QCOM TECHNOLOGY INC.	00:0D:F0:7D:BF:0C		
	Apple Inc	E4:CE:8F:CE:7D:AA		

Figure 40: Saving client scan results as network clients

11. Select “Save” to save the friendly names and descriptions

The data can be viewed and edited.

1. From the top menu bar, select “Manage | Network clients”
2. To change the information, select the MAC address or name
3. Right-click and select “Edit”
4. Edit the information
5. Select “Save”



Parameter	Current value	New Value
MAC Address:	00:1C:26:20:A0:60	00 :1C :26 :20 :A0 :60
Vendor:	Hon Hai Precision Ind. Co.,Ltd.	
MAC Alias:	00:1C:26:20:A0:60	00:1C:26:20:A0:60
User:		John Smith
Description:		Laptop

Figure 41: Editing network client

18.3.1 Adding a new client

1. From the top menu bar, select “Manage | Network clients”
2. In the hierarchical tree in the left pane, right-click the topmost element, titled “Network clients”
3. Select “Add”
4. Enter a MAC alias for the client
5. Enter a user’s name, if known
6. Enter a description (optional)
7. Enter the client’s MAC address
8. Click “Save”

To add several clients at once, select “Import network clients” in step 3. This option imports a text file from the Carat server’s file system. The file format is as follows:

field	MAC	Name	User	Description
explanation	MAC address, required	MAC alias, (optional)	Client user if known (optional)	Client description (optional)
example	complete	A:B:C:D,pda,Pda User, personal digital assistant		
	description omitted	A:B:C:D,officeLaptop,J.D.,		
	partial	A:B:C:D,barCodeReader, ,		

The “Export network clients” function creates a corresponding file in the Carat server’s file system.

18.4 Spectrum Analyzer[17]

The monitoring station supports frequency-sweep-based radio spectrum analysis. The frequency status is displayed as a colored map.

1. In the Network topology, select the Eye that will run the test
2. Right-click and select “Spectrum Analysis”
3. Select the test duration from the pull-down menu
4. Select the antennas to be used in the test by selecting their respective checkboxes
5. Select “Scan”

For the results, see the figure below:

[17] Not available in Soft and Micro Eyes

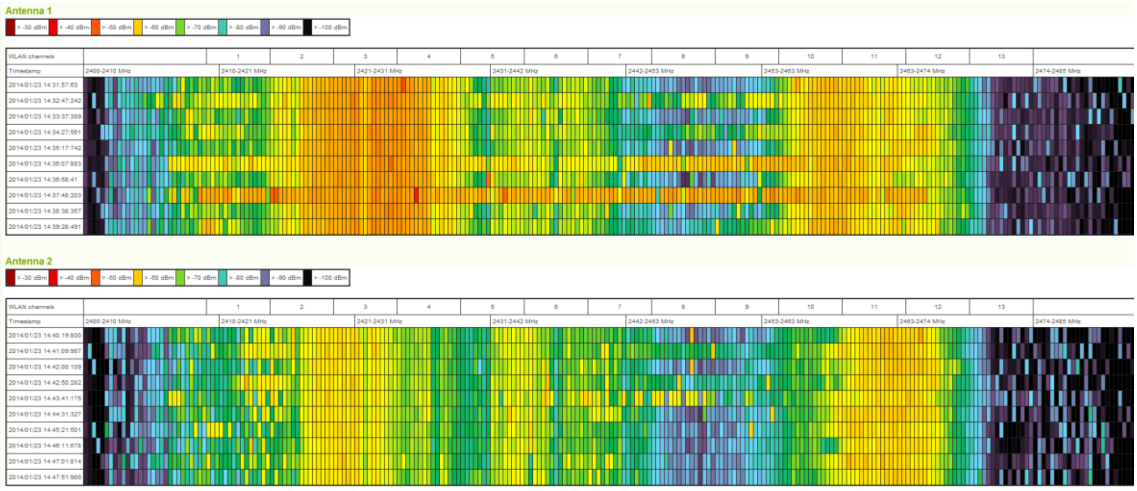


Figure 42: Spectrum analyzer result

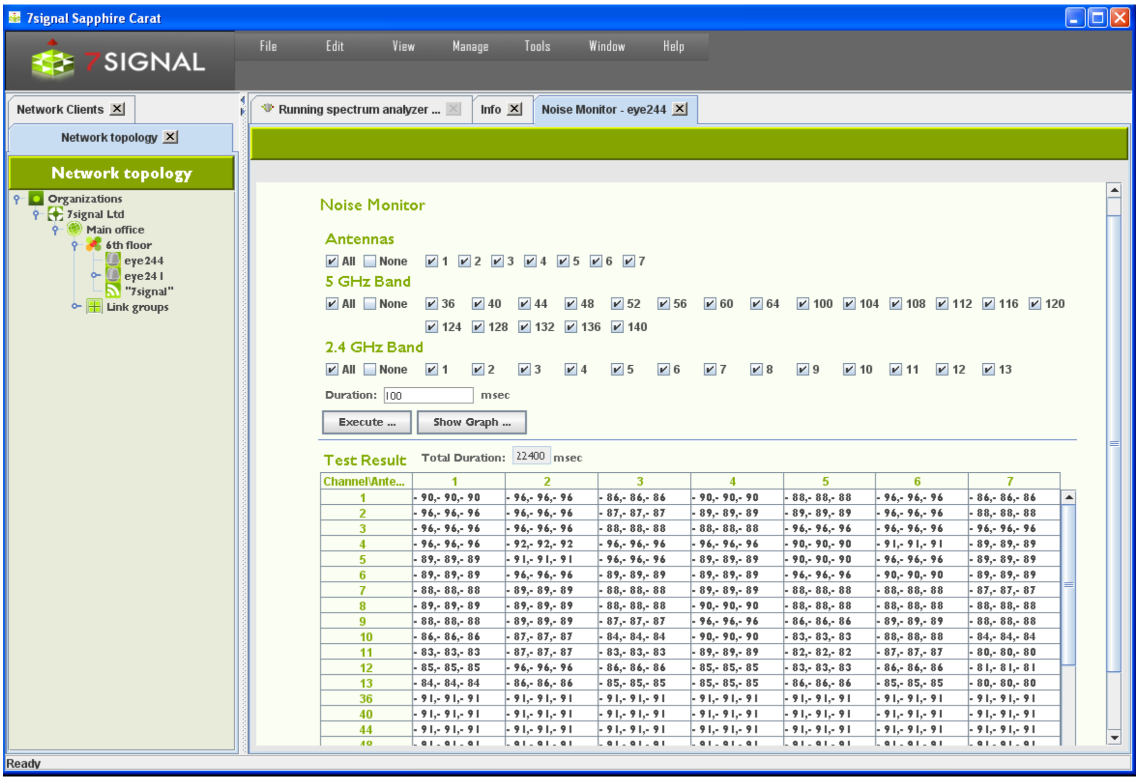
18.5 Noise monitor test[18]

You can measure the noise levels surrounding the monitoring station.

1. In the Network topology, select the Eye that will run the test
2. Right-click and select “Noise Monitor”
3. Select the scan directions – i.e., directional antennas[19]
4. Select the channels to scan
5. Select “Execute”
6. The results are displayed in a table as seen below
7. To view the results in a graphical view, click “Show graph”

[18] Might not be available in Soft and Micro Eyes. Noise reporting support depends on features of WLAN network interface.

[19] Only one antenna available in Soft and Micro Eyes



Noise Monitor

Antennas

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7

5 GHz Band

☑ All □ None ☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52 ☑ 56 ☑ 60 ☑ 64 ☑ 100 ☑ 104 ☑ 108 ☑ 112 ☑ 116 ☑ 120 ☑ 124 ☑ 128 ☑ 132 ☑ 136 ☑ 140

2.4 GHz Band

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13

Duration: 100 msec

Execute ... Show Graph ...

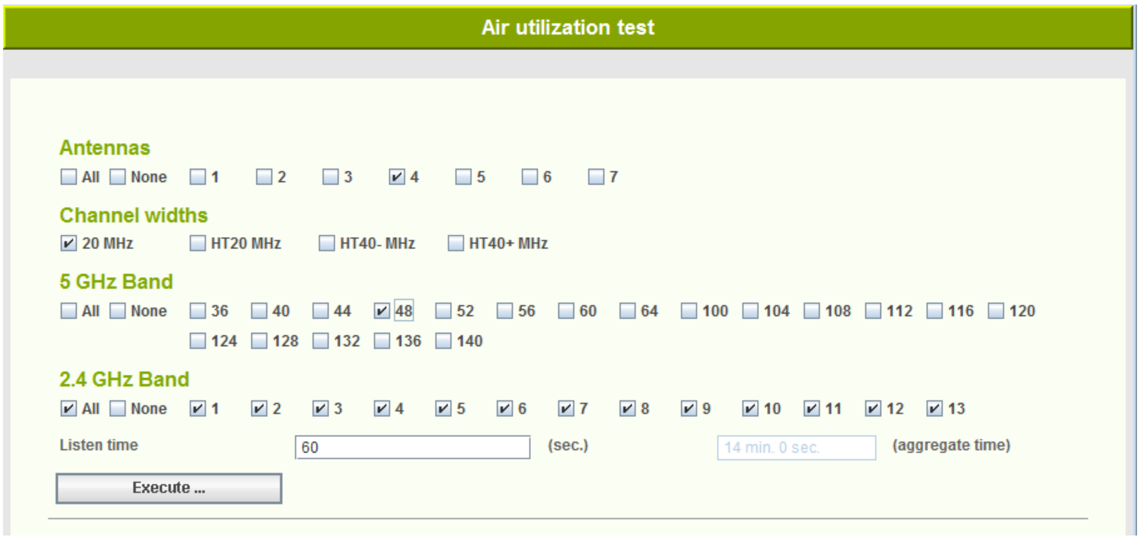
Test Result Total Duration: 22400 msec

Channel\Ante...	1	2	3	4	5	6	7
1	- 90,- 90,- 90	- 96,- 96,- 96	- 86,- 86,- 86	- 90,- 90,- 90	- 88,- 88,- 88	- 96,- 96,- 96	- 86,- 86,- 86
2	- 96,- 96,- 96	- 96,- 96,- 96	- 87,- 87,- 87	- 89,- 89,- 89	- 89,- 89,- 89	- 96,- 96,- 96	- 88,- 88,- 88
3	- 96,- 96,- 96	- 96,- 96,- 96	- 88,- 88,- 88	- 88,- 88,- 88	- 96,- 96,- 96	- 96,- 96,- 96	- 96,- 96,- 96
4	- 96,- 96,- 96	- 92,- 92,- 92	- 96,- 96,- 96	- 96,- 96,- 96	- 90,- 90,- 90	- 91,- 91,- 91	- 89,- 89,- 89
5	- 89,- 89,- 89	- 91,- 91,- 91	- 96,- 96,- 96	- 89,- 89,- 89	- 90,- 90,- 90	- 96,- 96,- 96	- 89,- 89,- 89
6	- 89,- 89,- 89	- 96,- 96,- 96	- 89,- 89,- 89	- 89,- 89,- 89	- 96,- 96,- 96	- 90,- 90,- 90	- 89,- 89,- 89
7	- 88,- 88,- 88	- 89,- 89,- 89	- 88,- 88,- 88	- 89,- 89,- 89	- 88,- 88,- 88	- 88,- 88,- 88	- 87,- 87,- 87
8	- 89,- 89,- 89	- 89,- 89,- 89	- 88,- 88,- 88	- 90,- 90,- 90	- 88,- 88,- 88	- 88,- 88,- 88	- 88,- 88,- 88
9	- 88,- 88,- 88	- 89,- 89,- 89	- 87,- 87,- 87	- 96,- 96,- 96	- 86,- 86,- 86	- 89,- 89,- 89	- 88,- 88,- 88
10	- 86,- 86,- 86	- 87,- 87,- 87	- 84,- 84,- 84	- 90,- 90,- 90	- 83,- 83,- 83	- 88,- 88,- 88	- 84,- 84,- 84
11	- 83,- 83,- 83	- 87,- 87,- 87	- 83,- 83,- 83	- 89,- 89,- 89	- 82,- 82,- 82	- 87,- 87,- 87	- 80,- 80,- 80
12	- 85,- 85,- 85	- 96,- 96,- 96	- 86,- 86,- 86	- 85,- 85,- 85	- 83,- 83,- 83	- 86,- 86,- 86	- 81,- 81,- 81
13	- 84,- 84,- 84	- 86,- 86,- 86	- 85,- 85,- 85	- 85,- 85,- 85	- 86,- 86,- 86	- 85,- 85,- 85	- 80,- 80,- 80
36	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91
40	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91
44	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91
48	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91	- 91,- 91,- 91

Figure 43: Noise monitor test

18.6 Air utilization test

To capture spectrum heavy-users and misconfigurations – such as extensive use of legacy codecs - in the WLAN network, air utilization test should be run. This test is not part of the default test profiles as it is lengthy troubleshoot test. Special attention to the test parameters is required as the maximum runtime is easily very high. One should check the “aggregate time” box for an estimate.



Air utilization test

Antennas

□ All □ None □ 1 □ 2 □ 3 ☑ 4 □ 5 □ 6 □ 7

Channel widths

☑ 20 MHz □ HT20 MHz □ HT40- MHz □ HT40+ MHz

5 GHz Band

□ All □ None □ 36 □ 40 □ 44 ☑ 48 □ 52 □ 56 □ 60 □ 64 □ 100 □ 104 □ 108 □ 112 □ 116 □ 120 □ 124 □ 128 □ 132 □ 136 □ 140

2.4 GHz Band

☑ All □ None ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13

Listen time 60 (sec.) 14 min. 0 sec. (aggregate time)

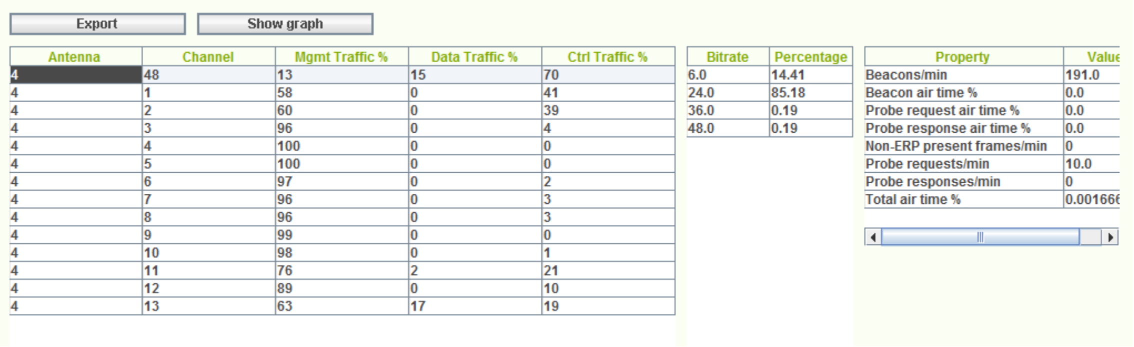
Execute ...

Figure 44: Air utilization test parameters

To run the test:

1. Select antennas, at least one must be selected.
2. Select channel width
3. Select the desired channels with the check-boxes.
4. Select the channel widths for the test (802.11n feature)
5. Select the time – in seconds – to listen to each selected channel on each selected antenna.

The results are shown in a table that has each antenna/channel combination as one row. By activating a row on the table with the mouse, detailed results about used bitrates and frame statistics are shown on the right side of the dialog.



Antenna	Channel	Mgmt Traffic %	Data Traffic %	Ctrl Traffic %
4	48	13	15	70
4	1	58	0	41
4	2	60	0	39
4	3	96	0	4
4	4	100	0	0
4	5	100	0	0
4	6	97	0	2
4	7	96	0	3
4	8	96	0	3
4	9	99	0	0
4	10	98	0	1
4	11	76	2	21
4	12	89	0	10
4	13	63	17	19

Bitrate	Percentage
6.0	14.41
24.0	85.18
36.0	0.19
48.0	0.19

Property	Value
Beacons/min	191.0
Beacon air time %	0.0
Probe request air time %	0.0
Probe response air time %	0.0
Non-ERP present frames/min	0
Probe requests/min	10.0
Probe responses/min	0
Total air time %	0.001666

Figure 45: Air utilization rest result

Graphical representation can be shown by clicking “Show graph” button:

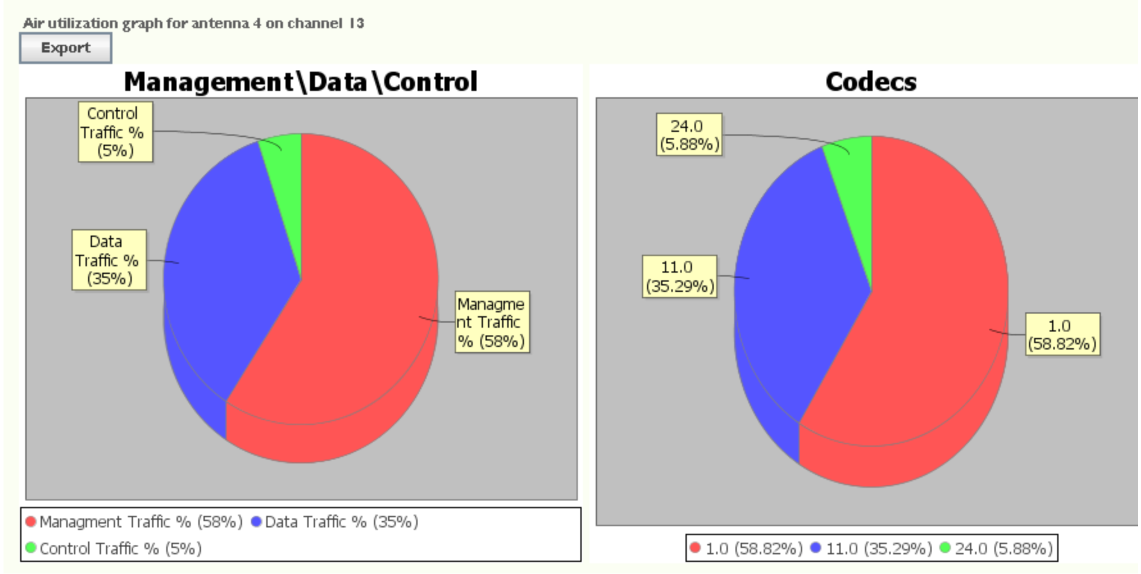

Air utilization graph for antenna 4 on channel 13

Figure 46: Air utilization test result graph

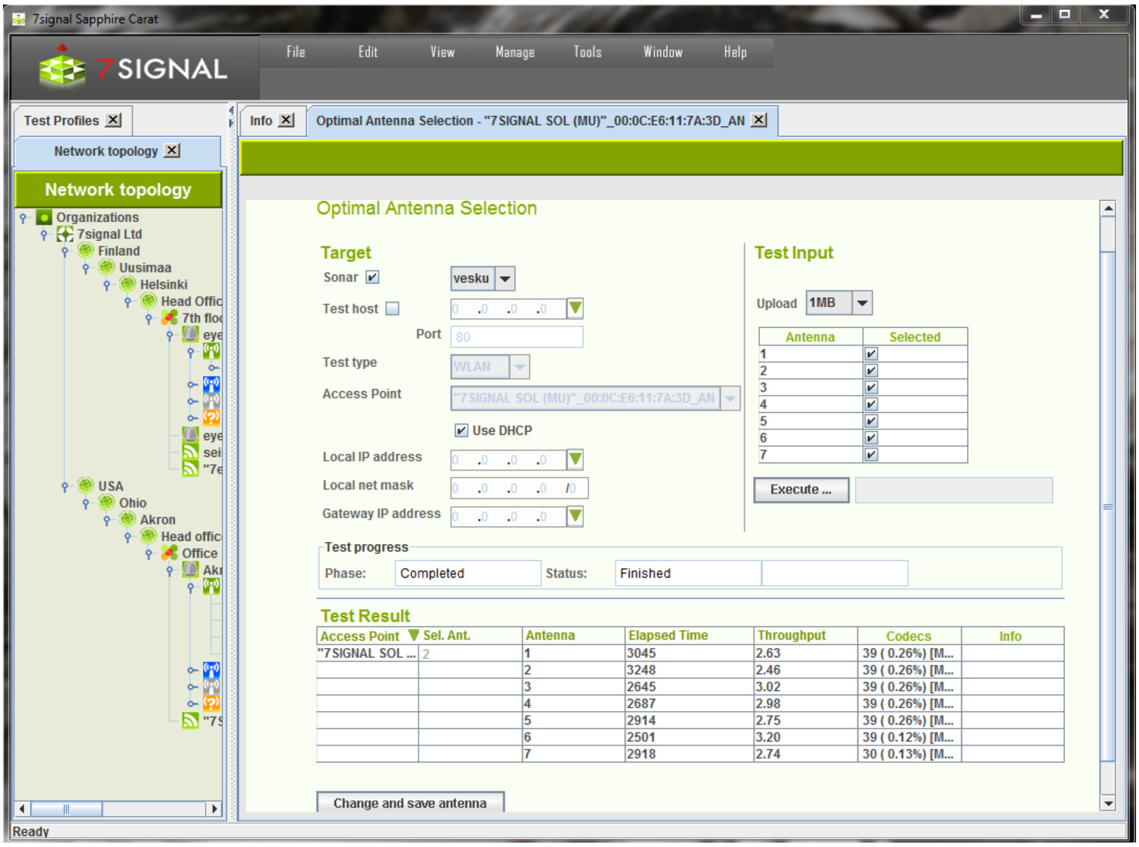
Antenna/channel row is presented in a pie-chart form that show frame type distribution on the left and codec distribution on the right.

18.7 Optimal antenna selection test[20]

The antenna test is used to verify the suitability of the selected antenna. Because of reflections, the network scan can show similar results for different antennas. However, during transmission of data to an access point, the differences between antennas become significant. This test is worth running if more than one antenna shows similar results.

1. In the Network topology, select
   a. the Eye that will run the test
      i. Right-click and select “Manual Tests | Optimal Antenna Selection”
      ii. Select an access point
   b. Or an access point through which the test will be run
      i. Right-click and select “Manual Tests | Optimal Antenna Selection”
2. Select the Sonar against which you want to run the test, or type another IP address
3. Select the Eye’s IP address (DHCP or static)
   a. If static, enter the (1) local IP address, (2) local net mask, and (3) gateway
4. Set up the test options:
   a. Select the amount of data transferred at one time
   b. Select the antennas to be used in the test
5. Select “Execute”. Test progress information can be seen in the “Test progress” area.
6. The results are displayed in a table as seen below
7. If an antenna gives better results than the currently used antenna, select the better antenna for monitoring. Select “Change and save antenna” to save the new antenna selection.

[20] Not available in Soft and Micro Eyes



Optimal Antenna Selection

Target

Sonar ☑ vesku

Test host □ 0 .0 .0 .0

Port 80

Test type WLAN

Access Point "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address 0 .0 .0 .0

Local net mask 0 .0 .0 .0 /0

Gateway IP address 0 .0 .0 .0

Test Input

Upload 1MB

Antenna	Selected
1	☑
2	☑
3	☑
4	☑
5	☑
6	☑
7	☑

Execute ...

Test progress

Phase: Completed Status: Finished

Test Result

Access Point	Sel. Ant.	Antenna	Elapsed Time	Throughput	Codecs	Info
"7SIGNAL SOL ...	2	1	3045	2.63	39 (0.26%) [M...	
		2	3248	2.46	39 (0.26%) [M...	
		3	2645	3.02	39 (0.26%) [M...	
		4	2687	2.98	39 (0.26%) [M...	
		5	2914	2.75	39 (0.26%) [M...	
		6	2501	3.20	39 (0.12%) [M...	
		7	2918	2.74	30 (0.13%) [M...	

Change and save antenna

Figure 47: Optimal antenna selection test

18.8 Download tests

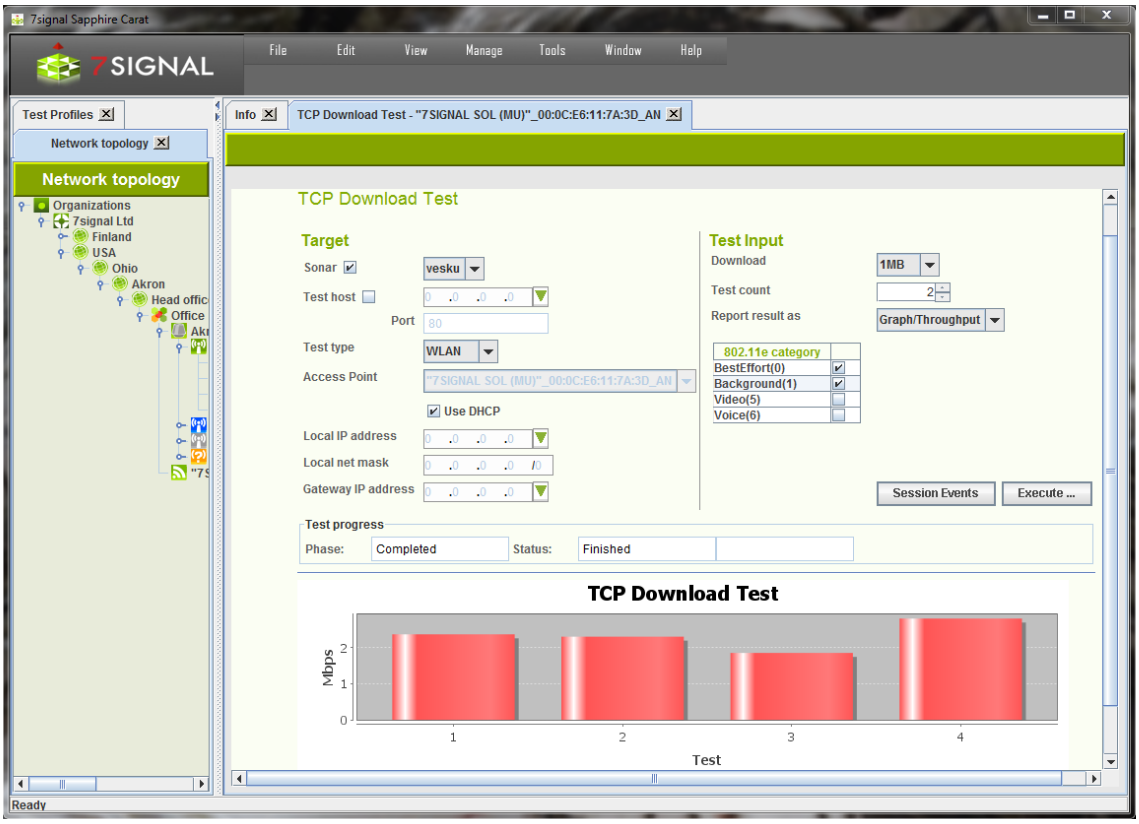
This test gives an indication of an access point's TCP or UDP downlink capacity.

1. In the Network topology, select
   a. the Eye that will run the test
      i. Right-click and select "Manual tests"
      ii. From the submenu select either "TCP Download Test" or "UDP Download Test"
      iii. Select an access point
   b. Or an access point through which the test will be run[21]
      i. Right-click and select "Manual tests"
      ii. From the submenu select either "TCP Download Test" or "UDP Download Test"
2. Specify whether you want to run the test against a Sonar or another target
3. Select the Sonar against which you want to run the test, or type another IP address
4. Select test type, WLAN or Ethernet
5. Select the Eye's IP address (DHCP or static)[22]
   a. If static, enter the (1) local IP address, (2) local net mask, and (3) gateway
6. Set up the test options
   a. Select the amount of data transferred at one time
   b. (UDP only): Packet size to be used (small = 256, medium = 1024, large = 32768 bytes)

[21] Meaningless if Ethernet test is chosen.
[22] Only if WLAN test is chosen.

   c. (UDP only): Sender (Sonar) port. Default 0 means that system shall allocate used ports. User-given port overrides this setting. Please observe possible firewall settings.
   d. (UDP only): Receiver (Eye) port. Default 0 means that system will allocate used ports. User-given port overrides this setting. Please observe possible firewall settings.
   e. Select the display format for the results
   f. Select how many times the test is to be run
7. Select "Execute". Test progress information can be seen in the "Test progress" area.
8. The results are displayed in a table as shown below

> You can change how the test result is shown even after the test is executed.



TCP Download Test - "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

TCP Download Test

Target

Sonar ☑ vesku

Test host ☐ 0 .0 .0 .0

Port 80

Test type WLAN

Access Point "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address 0 .0 .0 .0

Local net mask 0 .0 .0 .0 /0

Gateway IP address 0 .0 .0 .0

Test Input

Download 1MB

Test count 2

Report result as Graph/Throughput

802.11e category	
BestEffort(0)	☑
Background(1)	☑
Video(5)	☐
Voice(6)	☐

Test progress

Phase: Completed Status: Finished

Figure 48: TCP download test

18.9 Upload tests

This test gives an indication of an access point's TCP uplink capacity.

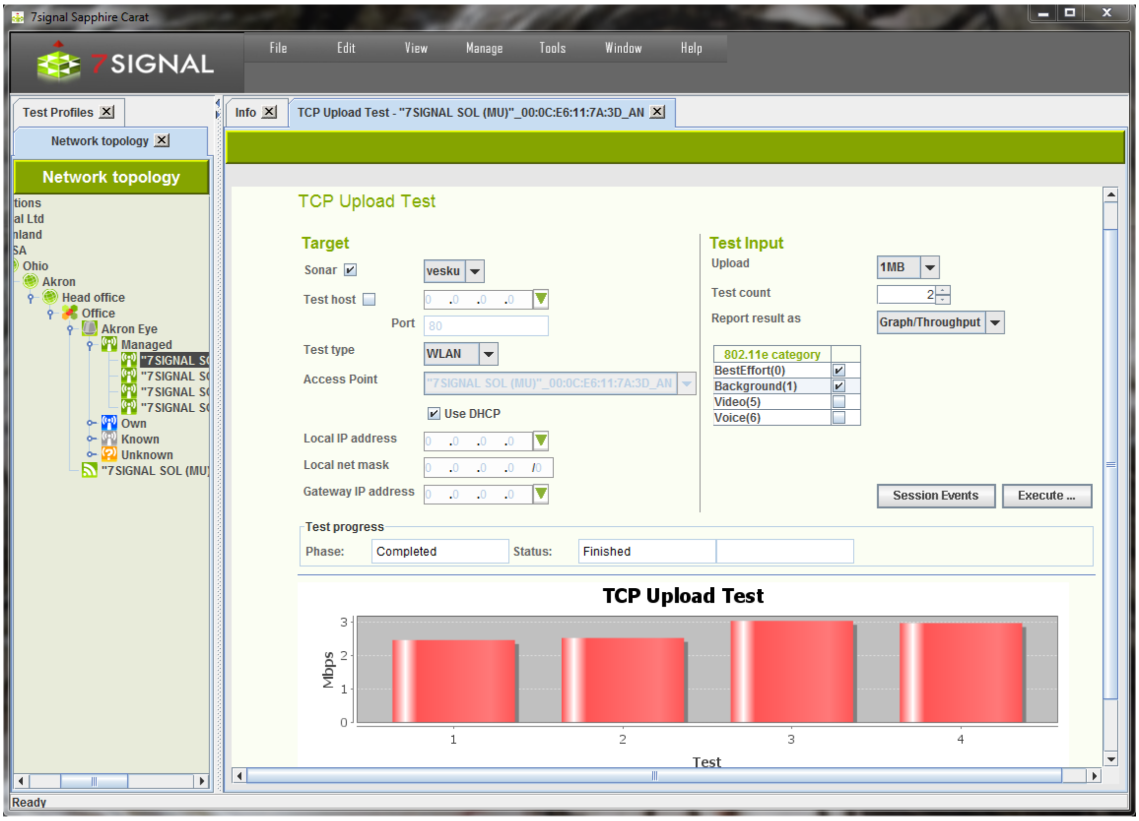
1. In the Network topology, select
   a. the Eye that will run the test
      i. Right-click and select "Manual tests"
      ii. From the submenu select either "TCP Upload Test" or "UDP Upload Test"
      iii. Select an access point from the pull-down menu

   b. Or an access point through which the test will be run[23]
      i. Right-click and select ”Manual tests”
      ii. From the submenu select either “TCP Upload Test” or “UDP Upload Test”
2. Select the Sonar against which you want to run the test, or type another IP address
3. Select test type, WLAN or Ethernet
4. Select the Eye’s IP address (DHCP or static)[24]
   a. If static, enter the (1) local IP address, (2) local net mask, and (3) gateway
5. Set up the test options:
   a. Select the amount of data from the pull-down menu
   b. (UDP only): Packet size to be used (small = 256, medium = 1024, large = 32768 bytes)
   c. (UDP only): Sender (Eye) port. Default 0 means that system will allocate ports .User-given port overrides this setting. Please observe possible firewall settings.
   d. (UDP only): Receiver (Sonar) port. Default 0 means that system shall allocate used ports. User-given port overrides this setting. Please observe possible firewall settings.
   e. Specify how many times the test is to be run
   f. Select the display format for the results from the pull-down menus
   g. Select the traffic classes to use (licensed products only)
6. Select “Execute”. Test progress information can be seen in the “Test progress” area.

The results are displayed in a table as seen below.

> You can change how the test results are shown even after the test is executed.

[23] Meaningless of Ethernet test is chosen.
[24] Only if WLAN test is chosen.



TCP Upload Test

Target

Sonar ☑ vesku

Test host □ 0 .0 .0 .0

Port 80

Test type WLAN

Access Point "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address 0 .0 .0 .0

Local net mask 0 .0 .0 .0 /0

Gateway IP address 0 .0 .0 .0

Test Input

Upload 1MB

Test count 2

Report result as Graph/Throughput

802.11e category	
BestEffort(0)	☑
Background(1)	☑
Video(5)	□
Voice(6)	□

Test progress

Phase: Completed Status: Finished

Figure 49: TCP upload test

18.10 Ping test

A ping test tests the accessibility of a device, the number of packets sent and received, and latency time.

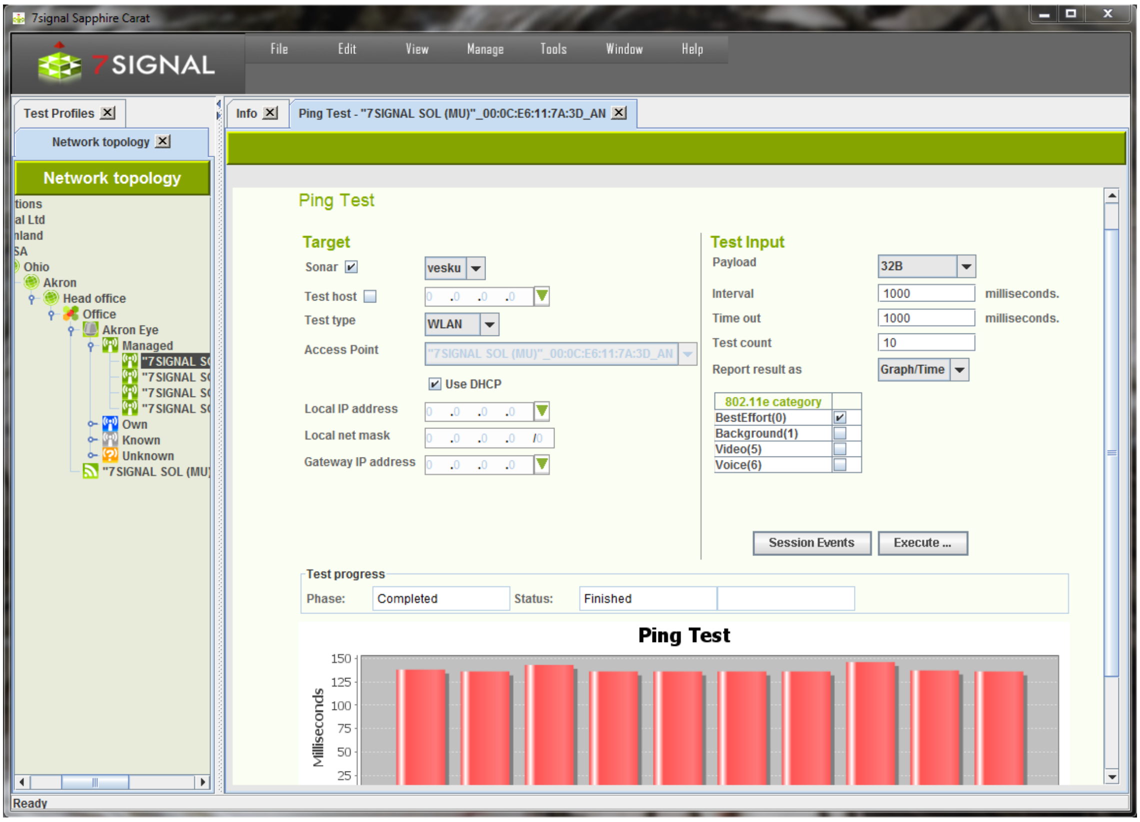
1. In the Network topology, select
   a. the Eye that will run the test
      i. Right-click and select ”Manual tests | Ping test”
      ii. Select an access point from the pull-down menu
   b. Or an access point through which the test will be run[25]
      i. Right-click and select ”Manual tests | Ping Test”
2. Select the Sonar against which you want to run the test, or type another IP address
3. Select test type, WLAN or Ethernet
4. Select the Eye’s IP address (DHCP or static)[26]
   a. If static, enter the (1) local IP address, (2) local net mask, and (3) gateway

5. Set up the test options:
   a. Select the size for the ping packet
   b. Select the waiting time between ping tests (in milliseconds)
   c. Select the waiting time (in seconds) before termination of a test that does not progress
   d. Specify how many pings will be send.
   e. Select the display format for the results from the pull-down menus
6. Select the traffic classes to use (licensed products only) – *note that it is not recommended to use traffic classes in a ping test*

[25] Meaningless if Ethernet test is chosen
[26] Only if WLAN test is chosen.

7. Select “Execute”. Test progress information can be seen in the “Test progress” area. The results are displayed in a report as seen below.

> You can change how the test results are shown even after the test is executed.



Ping Test

Target

Sonar ☑ vesku

Test host □ 0 .0 .0 .0

Test type WLAN

Access Point "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address 0 .0 .0 .0

Local net mask 0 .0 .0 .0 /0

Gateway IP address 0 .0 .0 .0

Test Input

Payload 32B

Interval 1000 milliseconds.

Time out 1000 milliseconds.

Test count 10

Report result as Graph/Time

802.11e category	
BestEffort(0)	☑
Background(1)	□
Video(5)	□
Voice(6)	□

Test progress

Phase: Completed Status: Finished

Figure 50: Ping test

18.11 Trace route test

This test helps one perform network troubleshooting and identify routing problems or firewalls that may be blocking access to a host.

1. In the Network topology, select
   a. the Eye that will run the test
      i. Right-click and select ”Manual tests | Traceroute Test”
      ii. Select an access point from the pull-down menu
   b. Or an access point through which the test will be run[27]
      i. Right-click and select ”Manual tests | Traceroute Test”
2. Select the Sonar against which you want to run the test, or type another IP address
3. Select test type, WLAN or Ethernet
4. Select the Eye’s IP address (DHCP or static)[28]
   a. If static, enter the (1) local IP address, (2) local net mask, and (3) gateway
5. Set up the test options:
   a. Minimum TTL: minimum number of devices/hops to try

[27] Meaningless if Ethernet test is chosen.

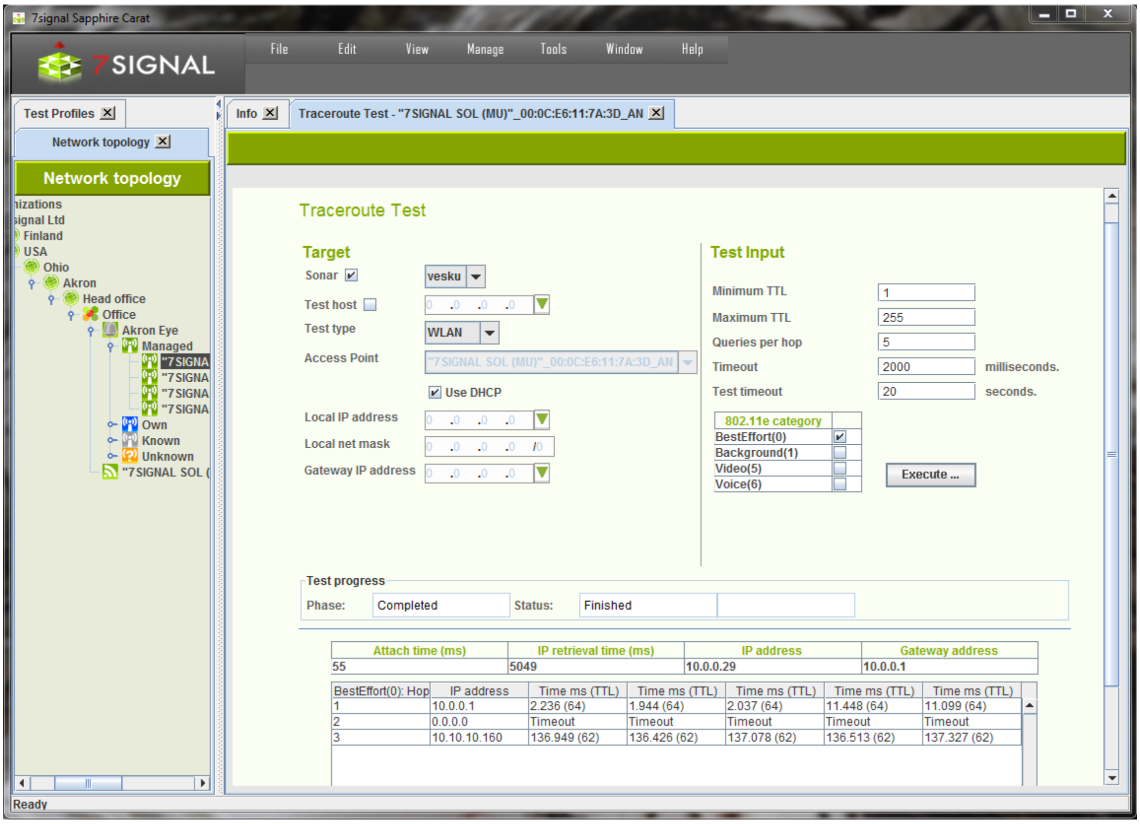
[28] Only if WLAN test is chosen.

   b. Maximum TTL: maximum number of devices/hops to try
   c. Queries per hop: how many times a device/hop is tried
   d. Timeout: how long to wait before giving up on a device/hop
   e. Test timeout: how long the test is allowed to be run at maximum (useful if there is a risk that the destination Sonar is unreachable)

6. Select the traffic classes to use (licensed products only)
7. Select "Execute". Test progress information can be seen in "Test progress" area

The results are displayed in a report as seen below.

Note: You can change the report type even after the test is executed



Traceroute Test

Target

Sonar ☑ vesku

Test host ☐ 0 .0 .0 .0

Test type WLAN

Access Point "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address 0 .0 .0 .0

Local net mask 0 .0 .0 .0 /0

Gateway IP address 0 .0 .0 .0

Test Input

Minimum TTL 1

Maximum TTL 255

Queries per hop 5

Timeout 2000 milliseconds.

Test timeout 20 seconds.

802.11e category	
BestEffort(0)	☑
Background(1)	☐
Video(5)	☐
Voice(6)	☐

Test progress

Phase: Completed Status: Finished

Attach time (ms)	IP retrieval time (ms)	IP address	Gateway address
55	5049	10.0.0.29	10.0.0.1

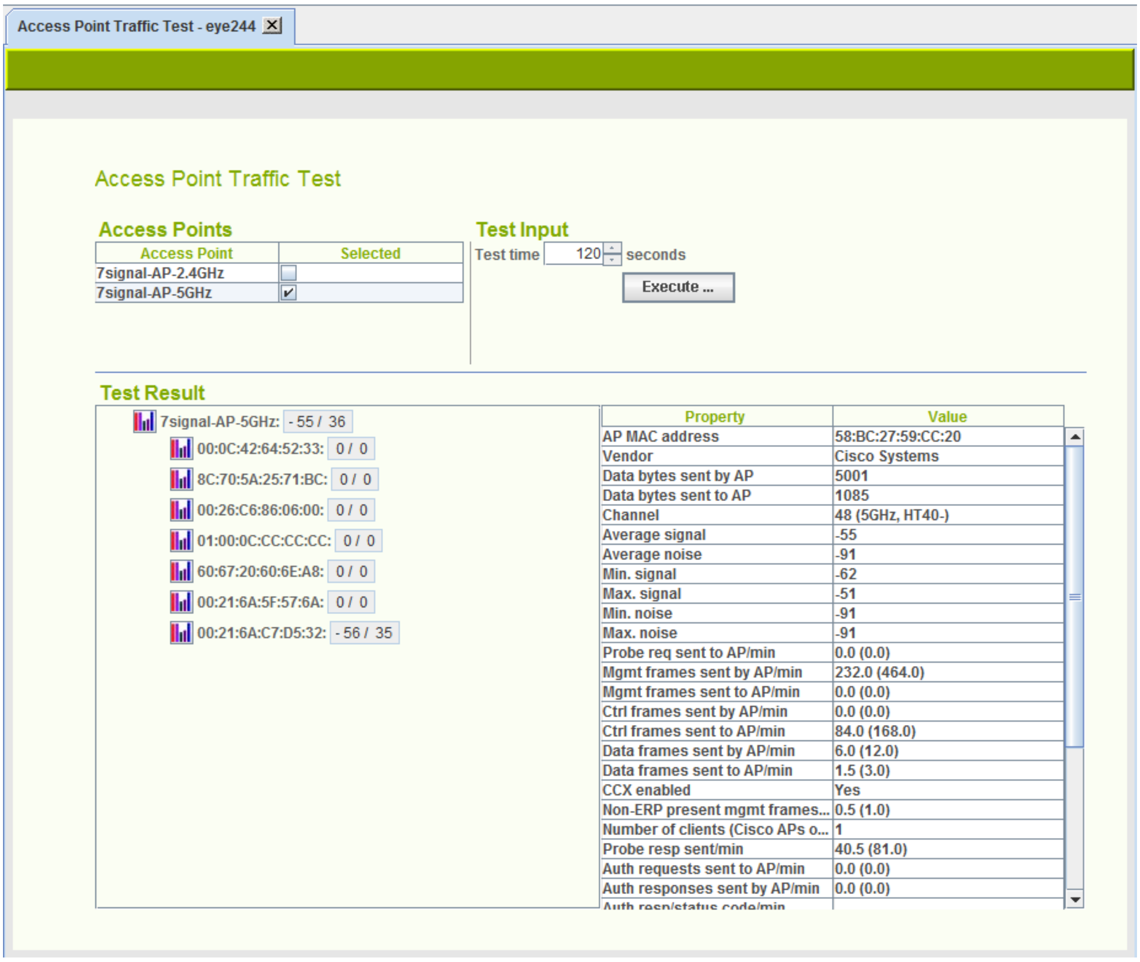
BestEffort(0): Hop	IP address	Time ms (TTL)	Time ms (TTL)	Time ms (TTL)	Time ms (TTL)	Time ms (TTL)
1	10.0.0.1	2.236 (64)	1.944 (64)	2.037 (64)	11.448 (64)	11.099 (64)
2	0.0.0.0	Timeout	Timeout	Timeout	Timeout	Timeout
3	10.10.10.160	136.949 (62)	136.426 (62)	137.078 (62)	136.513 (62)	137.327 (62)

Figure 51: Traceroute test

18.12 Access point traffic test

This test listens to radio traffic in the Sapphire Eye's coverage area and gathers many kinds of information.

1. In the Network topology, select the Eye that will run the test
2. Right-click and select "Manual tests | Access Point Traffic Test"
   Note: This test is among the active tests since it requires you to select a target access point
3. Select the target access points from the table
4. Select the listening time (in seconds)
5. Select "Execute"



Access Point Traffic Test - eye244 ☒

Access Point Traffic Test

Access Points

Access Point	Selected
7signal-AP-2.4GHz	□
7signal-AP-5GHz	☑

Test Input

Test time 120 seconds

Execute ...

Test Result

- 7signal-AP-5GHz: - 55 / 36
  - 00:0C:42:64:52:33: 0 / 0
  - 8C:70:5A:25:71:BC: 0 / 0
  - 00:26:C6:86:06:00: 0 / 0
  - 01:00:0C:CC:CC:CC: 0 / 0
  - 60:67:20:60:6E:A8: 0 / 0
  - 00:21:6A:5F:57:6A: 0 / 0
  - 00:21:6A:C7:D5:32: - 56 / 35

Property	Value
AP MAC address	58:BC:27:59:CC:20
Vendor	Cisco Systems
Data bytes sent by AP	5001
Data bytes sent to AP	1085
Channel	48 (5GHz, HT40-)
Average signal	-55
Average noise	-91
Min. signal	-62
Max. signal	-51
Min. noise	-91
Max. noise	-91
Probe req sent to AP/min	0.0 (0.0)
Mgmt frames sent by AP/min	232.0 (464.0)
Mgmt frames sent to AP/min	0.0 (0.0)
Ctrl frames sent by AP/min	0.0 (0.0)
Ctrl frames sent to AP/min	84.0 (168.0)
Data frames sent by AP/min	6.0 (12.0)
Data frames sent to AP/min	1.5 (3.0)
CCX enabled	Yes
Non-ERP present mgmt frames...	0.5 (1.0)
Number of clients (Cisco APs o...	1
Probe resp sent/min	40.5 (81.0)
Auth requests sent to AP/min	0.0 (0.0)
Auth responses sent by AP/min	0.0 (0.0)
Auth resp/status code/min	

Figure 52: Access point traffic test

The results are displayed in a table as seen above – the tree view in the table shows the access point as the root node, and the heard clients under it; for more information, move the mouse cursor over the individual items in the tree or, to display even more details and a graphical view, click an item in the tree.

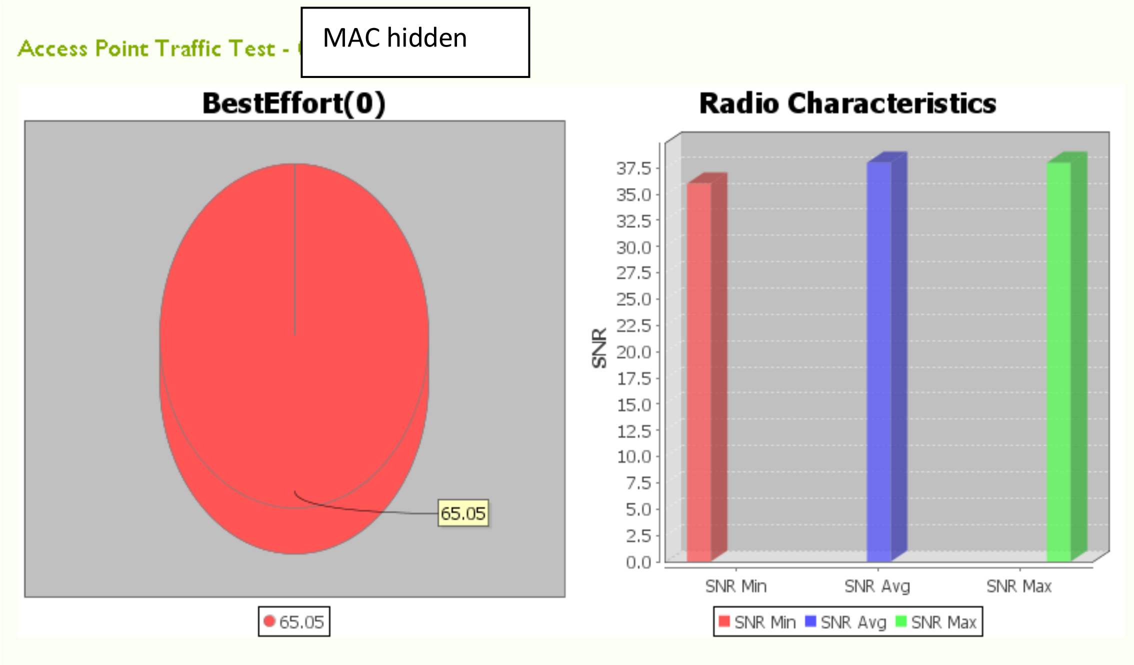
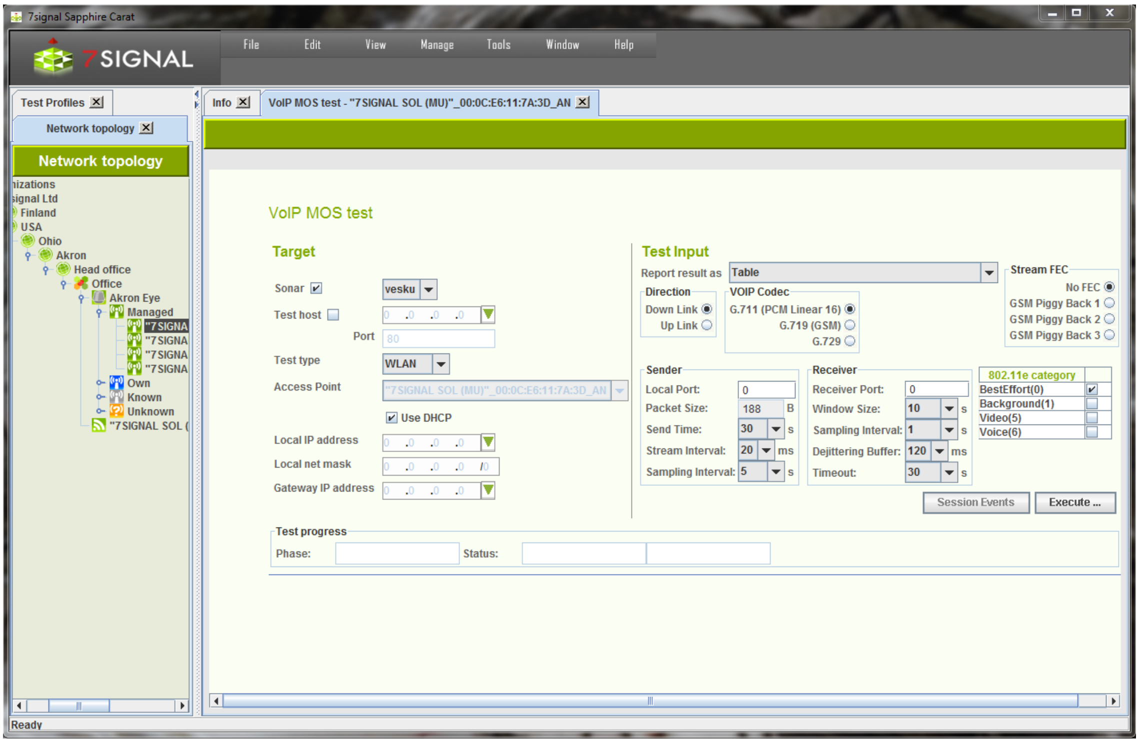


Figure 53: Access point traffic - client codec and radio characteristics

18.13 MOS test

This test creates a VoIP call between Sapphire Eye and Sonar. Both uplink and downlink call quality can be measured.

1. In the Network topology, select
    a. the Eye that will run the test
        i. Right-click and select ”Manual tests | VoIP MOS test”
        ii. Select an access point from the pull-down menu
    b. Or an access point through which the test will be run[29]
        i. Right-click and select ”Manual tests | VoIP MOS Test”
2. Select the Sonar against which you want to run the test
3. Select test type, WLAN or Ethernet
4. Select the Eye’s IP address (DHCP or static)[30]
    a. If static, enter the (1) local IP address, (2) local net mask, and (3) gateway
5. Configure the test data (see separate instructions)
6. Select “Execute”. Test progress information can be seen in “Test progress” area



VoIP MOS test - "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

VoIP MOS test

Target

Sonar ☑ vesku

Test host □ 0 .0 .0 .0

Port 80

Test type WLAN

Access Point "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address 0 .0 .0 .0

Local net mask 0 .0 .0 .0 /0

Gateway IP address 0 .0 .0 .0

Test Input

Report result as Table

Direction: Down Link ● Up Link ○

VOIP Codec: G.711 (PCM Linear 16) ● G.719 (GSM) ○ G.729 ○

Stream FEC: No FEC ● GSM Piggy Back 1 ○ GSM Piggy Back 2 ○ GSM Piggy Back 3 ○

Sender

Local Port: 0

Packet Size: 188 B

Send Time: 30 s

Stream Interval: 20 ms

Sampling Interval: 5 s

Receiver

Receiver Port: 0

Window Size: 10 s

Sampling Interval: 1 s

Dejittering Buffer: 120 ms

Timeout: 30 s

802.11e category	
BestEffort(0)	☑
Background(1)	□
Video(5)	□
Voice(6)	□

Session Events   Execute ...

Test progress

Phase: Status:

Figure 54: VoIP MOS test

18.13.1 MOS test parameters

1. Select the initial display format for the results (Table/Graph)
2. Select the direction of the test (Downlink/Uplink)
3. Select the codec to be used in the test (VoIP Codec):
    a. G.711 PCM Linear 16 = 64 kbit/s
    b. G.729 GSM data = 8 kbit/s
4. Select an optional error correction method (Stream FEC)

[29] Meaningless if Ethernet test is chosen.
[30] Only if WLAN test is chosen.

5. Configure sender information:
    a. Enter a port for the MOS test (Local port, 0 means port allocated by the system)
    b. Enter the test duration in seconds (Send time)
    c. Enter the packet interval in milliseconds (Stream interval)
    d. Enter the packet size in bytes (Packet size)
    e. Enter the sampling window size in seconds (Sampling interval)
6. Configure the receiver information:
    a. Enter a port for the MOS test (Receiver port, 0 means port allocated by the system)
    b. Enter the receiving window size in seconds (Window size)
    c. Enter the sampling interval in seconds (Sampling Interval)
    d. Enter the size of the dejittering buffer (Dejittering Buffer)
    e. Enter the connection timeout in milliseconds (Timeout)
7. Enter the traffic class (licensed feature only)
8. Select "Execute". Test progress information can be seen in "Test progress" area.
9. The results are displayed in a new window in the selected format

18.13.2 MOS test result

Sample result set:

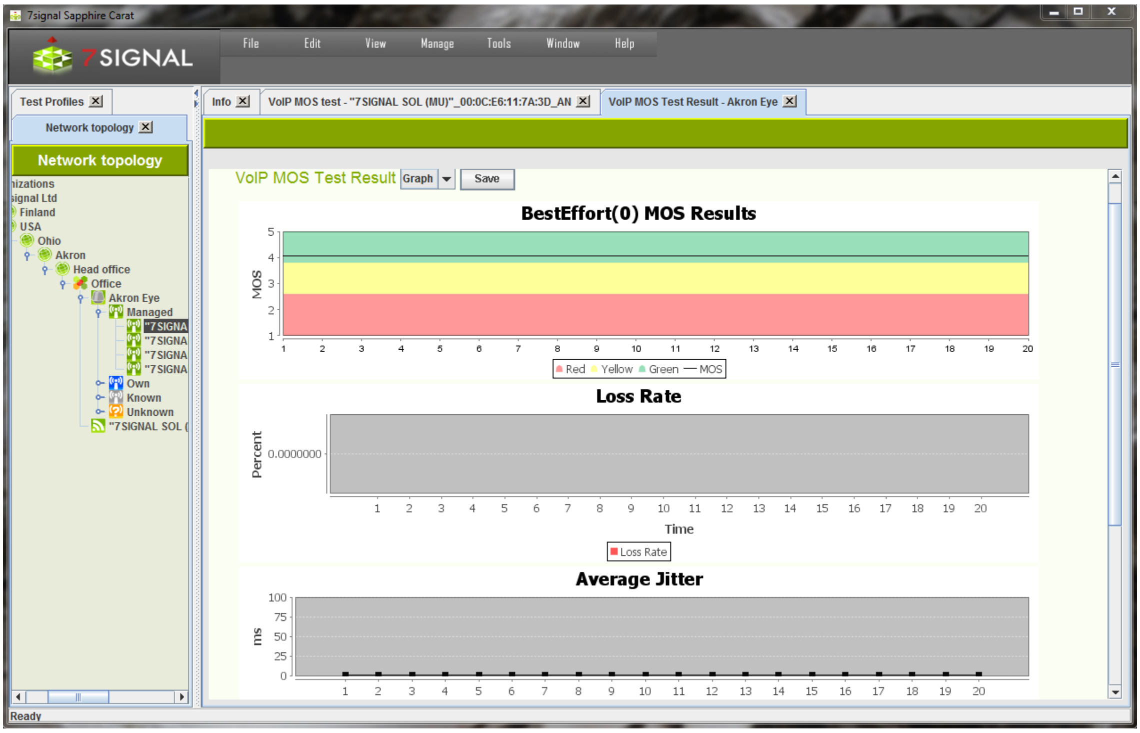


Figure 55: VoIP MOS test result graphs (top)

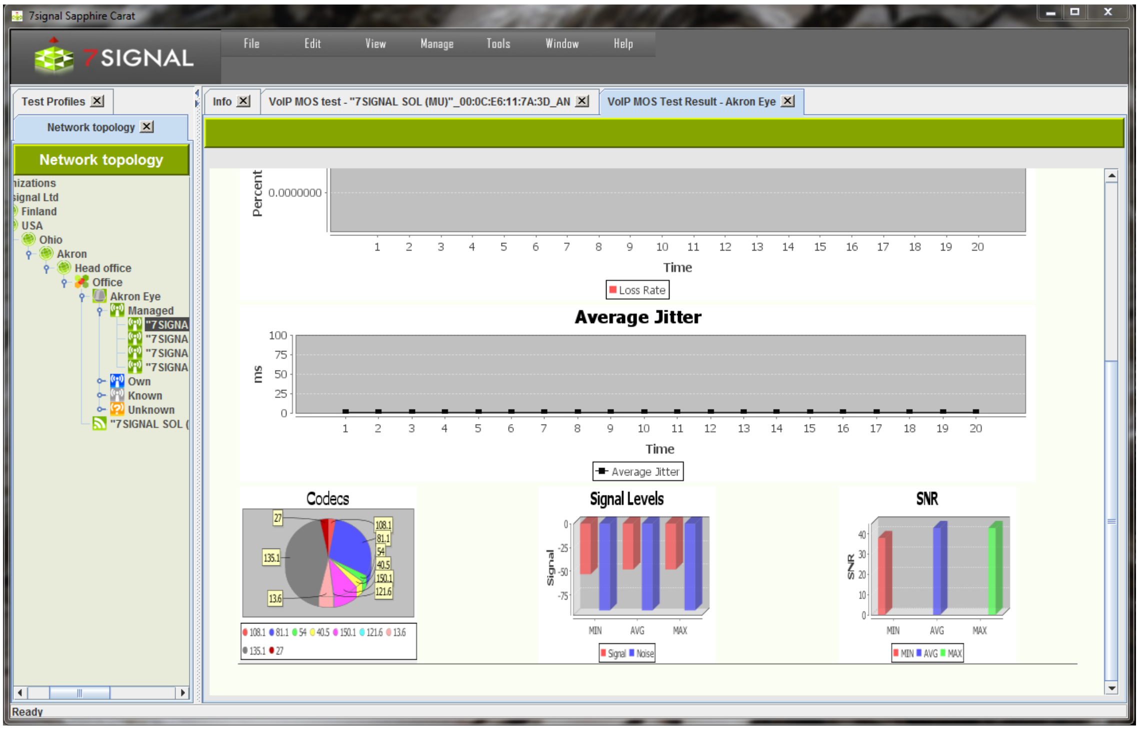


Figure 56: VoIP MOS test result graphs (bottom)

Elements of the results image:

- **MOS result:** The distribution of MOS values related to test duration. The color coding indicates quality.
- **Loss Rate:** Packet loss as a function of test duration.
- **Average Jitter:** Variation in delay as a function of test duration.
- **Codec:** The distribution of codecs used during the test. If only one result is visible, the codec was not changed during the test.
- **Levels:** Signal and noise levels during the test, averaged over the duration of the test.
- **SNR:** Signal/noise ratio during the test, averaged over the duration of the test.

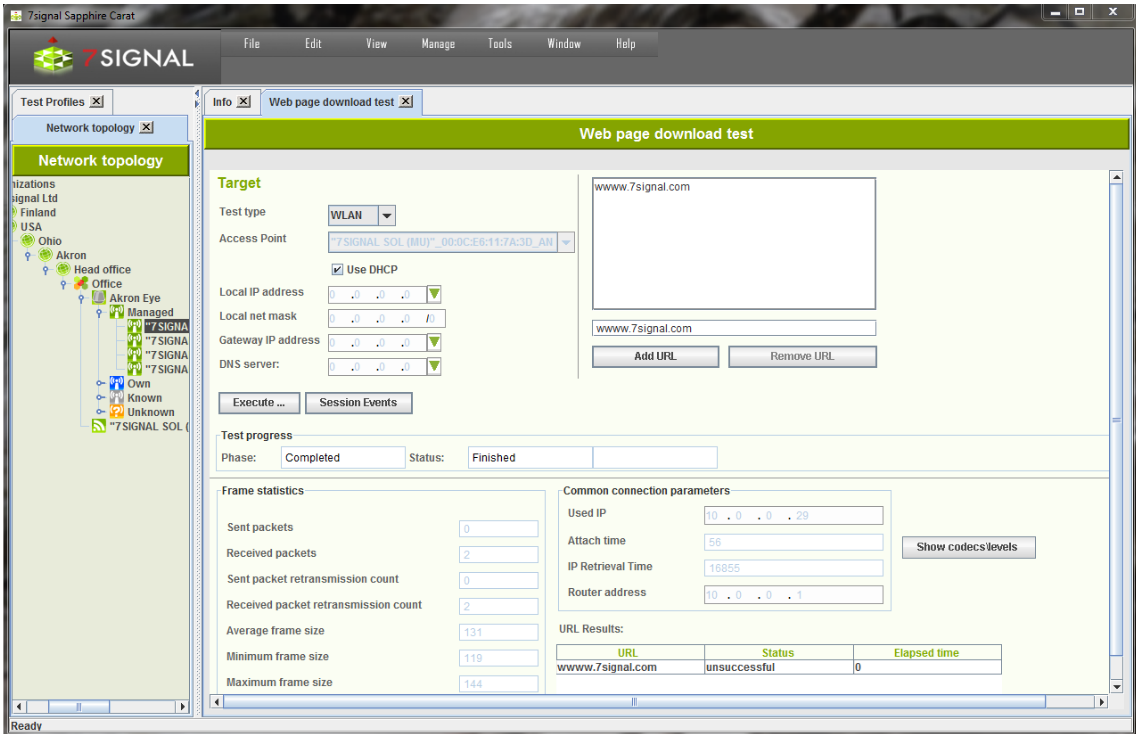
Table 12: MOS values

Test result	
5	Excellent
4	Good
3	Fair
2	Poor
1	Bad

In practice, the supported codec's can reach MOS scores that are slightly above 4.

18.14 Web page download test

This test is used for “downloading” actual WWW-pages.



Web page download test

Target

Test type: WLAN

Access Point: "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address: 0 .0 .0 .0

Local net mask: 0 .0 .0 .0 /0

Gateway IP address: 0 .0 .0 .0

DNS server: 0 .0 .0 .0

wwww.7signal.com

www.7signal.com

Test progress

Phase: Completed Status: Finished

Frame statistics

Sent packets: 0

Received packets: 2

Sent packet retransmission count: 0

Received packet retransmission count: 2

Average frame size: 131

Minimum frame size: 119

Maximum frame size: 144

Common connection parameters

Used IP: 10 . 0 . 0 . 29

Attach time: 56

IP Retrieval Time: 16855

Router address: 10 . 0 . 0 . 1

URL Results:

URL	Status	Elapsed time
wwww.7signal.com	unsuccessful	0

Figure 57: Web page download test

To run the web page download test:

1. In the Network topology, select
    a. the Eye that will run the test
        i. Right-click and select ”Manual tests | Web page download test”
        ii. Select an access point from the pull-down menu
    b. Or an access point through which the test will be run[31]
        i. Right-click and select ”Manual tests | Web page download test”
2. Select test type, WLAN or Ethernet
    a. If Ethernet test is chosen, DNS server IP address must be entered manually
3. Select the Eye’s IP address (DHCP or static)[32]
    a. If static, enter the (1) local IP address, (2) local net mask, (3) gateway, (4) DNS server IP address
4. Choose URL from the box
    a. To add a URL
        i. Write a well-formed and proper address to the input box
        ii. Select “Add URL”
    b. To remove a URL
        i. Activate the URL to be removed with a right-click
        ii. Select “Remove URL”
5. Select “Execute”. Test progress information can be seen in “Test progress” area.

[31] Meaningless if Ethernet test is chosen.
[32] Only if WLAN test is chosen.

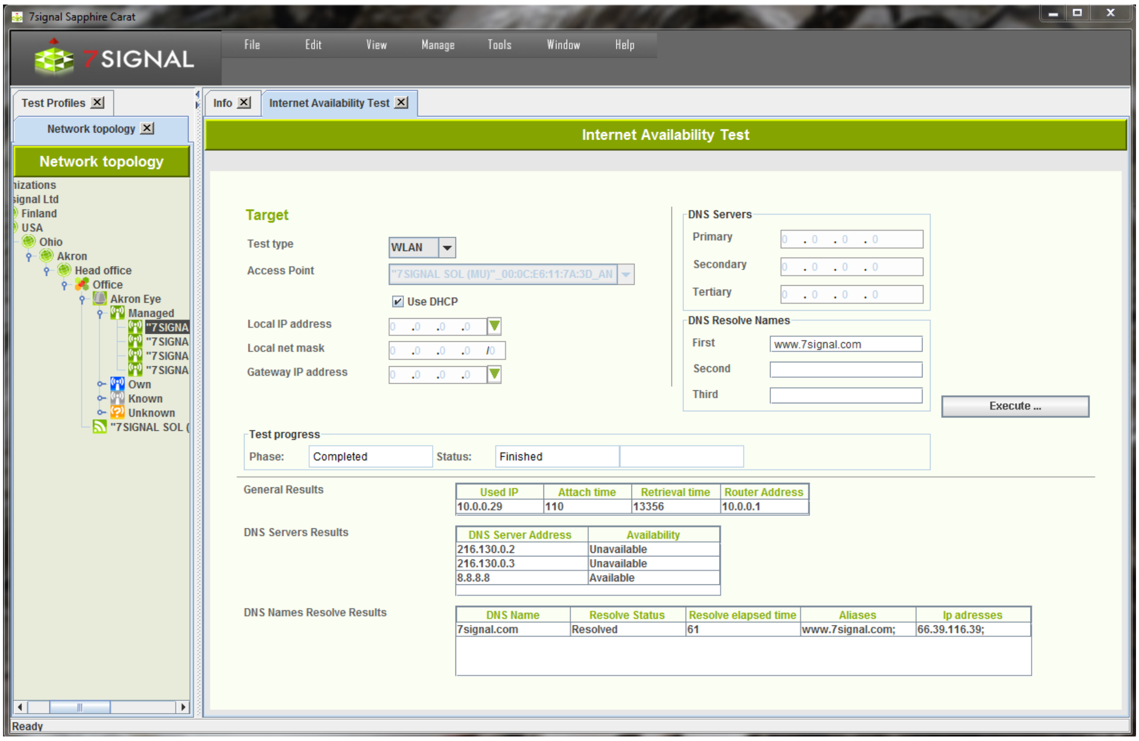
The result marks whether the download was successful (protocol errors or not), the download time and the downloaded byte count.

18.15 Internet Availability test

This is an infrastructure test that reflects how well a WLAN or Ethernet client (Eye monitoring station) is able to utilize the Internet. The test includes the following steps:

- radio link setup (WLAN only)
- WLAN authentication (WLAN only)
- DHCP service (WLAN only)
- Gateway pinging
- DNS server checks
- DNS name resolves

If the monitoring station passes all the phases of the test, it is justified to assume that the internet use is in general fully functional.



Internet Availability Test

Target

Test type: WLAN

Access Point: "7SIGNAL SOL (MU)"_00:0C:E6:11:7A:3D_AN

☑ Use DHCP

Local IP address: 0 .0 .0 .0

Local net mask: 0 .0 .0 .0 /0

Gateway IP address: 0 .0 .0 .0

DNS Servers

Primary: 0 . 0 . 0 . 0

Secondary: 0 . 0 . 0 . 0

Tertiary: 0 . 0 . 0 . 0

DNS Resolve Names

First: www.7signal.com

Second:

Third:

Test progress

Phase: Completed Status: Finished

General Results

Used IP	Attach time	Retrieval time	Router Address
10.0.0.29	110	13356	10.0.0.1

DNS Servers Results

DNS Server Address	Availability
216.130.0.2	Unavailable
216.130.0.3	Unavailable
8.8.8.8	Available

DNS Names Resolve Results

DNS Name	Resolve Status	Resolve elapsed time	Aliases	Ip adresses
7signal.com	Resolved	61	www.7signal.com;	66.39.116.39;

Figure 58: Internet availability test

To run the Internet availability test:

1. In the Network topology, select
   a. the Eye that will run the test
      i. Right-click and select ”Manual tests | Internet Availability test”
      ii. Select an access point from the pull-down menu
   b. Or, directly, an access point through which the test will be run[33]
      i. Right-click and select ”Manual tests | Internet Availability test”
2. Select test type, WLAN or Ethernet

[33] Meaningless if Ethernet test is chosen.

3. Select IP address
    a. Use DHCP of the WLAN network by checking the box[34]
        i. DHCP result shall affect other test parameters as the actual servers shall be dictated by the result and the reliability is expected.
    b. Use of static IP address configuration
        i. enter the (1) local IP address, (2) local net mask, and (3) gateway
        ii. Enter primary DNS server[35]
        iii. Enter secondary DNS server (optional)
        iv. Enter tertiary DNS server (optional)
    c. Enter 1st network name to be resolved
    d. Enter 2nd network name to be resolved (optional)
    e. Enter 3rd network name to be resolved (optional)
4. Select “Execute”. Test progress information can be seen in “Test progress” area.

The result-set is three-fold:

1. General results: IP address obtained, attach time, DHCP retrieval time and gateway address.
2. Status of DNS servers
3. Results of the name resolving.

18.16 SIP Register test

It is possible to run SIP Register test in both unauthorized and authorized mode.

To run the SIP test:

1. In the Network topology, select
    a. the Eye that will run the test
        i. Right-click and select ”Manual tests | SIP Registration Test”
        ii. Select an access point from the pull-down menu
    b. Or an access point through which the test will be run[36]
        i. Right-click and select ”Manual tests | SIP Registration Test”
2. Select the SIP server to register to
    a. From the pull-down menu
        i. SIP end-point has to be defined as a test end-point to be selectable
    b. Arbitrary IP address
        i. Enter IP address and the port
3. Select test type, WLAN or Ethernet
4. Select an access point[37]
5. Select the Eye’s IP address (DHCP or static)[38]
    a. If static, enter the (1) local IP address, (2) local net mask, and (3) gateway
6. Enter the SIP protocol specific parameters
    a. Name is mandatory
    b. If alone, the test is run as un-authorized
7. Select the WLAN traffic category[39]
8. Select “Execute”. Test progress information can be seen in “Test progress” area.

[34] Only if WLAN test is chosen.

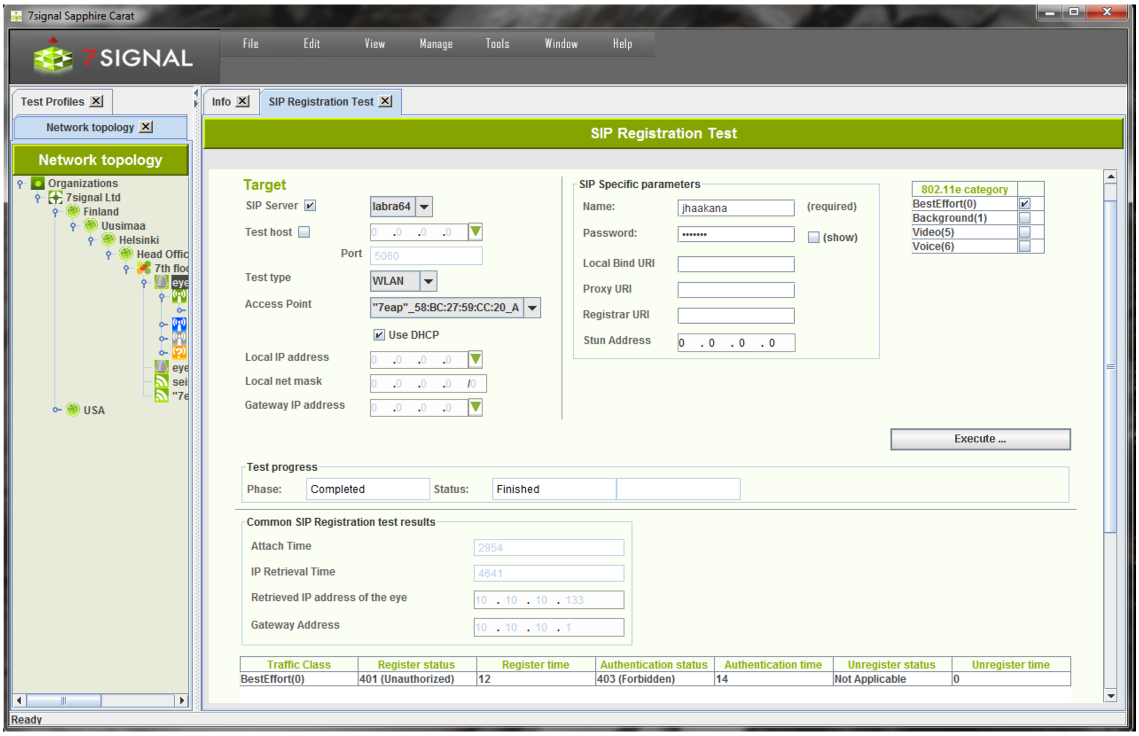
[35] Entering DNS servers are mandatory if Ethernet test is chosen.

[36] Meaningless if Ethernet test is chosen.

[37] Meaningless if Ethernet test is chosen.

[38] Only if WLAN test is chosen.

[39] Only if WLAN test is chosen.



SIP Registration Test

Target

SIP Server ☑ labra64
Test host □ 0 .0 .0 .0
Port 5060
Test type WLAN
Access Point "7eap"_58:BC:27:59:CC:20_A
☑ Use DHCP
Local IP address 0 .0 .0 .0
Local net mask 0 .0 .0 .0 /0
Gateway IP address 0 .0 .0 .0

SIP Specific parameters

Name: jhaakana (required)
Password: ••••••• □ (show)
Local Bind URI
Proxy URI
Registrar URI
Stun Address 0 . 0 . 0 . 0

802.11e category	
BestEffort(0)	☑
Background(1)	□
Video(5)	□
Voice(6)	□

Test progress

Phase: Completed Status: Finished

Common SIP Registration test results

Attach Time 2954
IP Retrieval Time 4641
Retrieved IP address of the eye 10 . 10 . 10 . 133
Gateway Address 10 . 10 . 10 . 1

Traffic Class	Register status	Register time	Authentication status	Authentication time	Unregister status	Unregister time
BestEffort(0)	401 (Unauthorized)	12	403 (Forbidden)	14	Not Applicable	0

Figure 59: SIP register test

The test result is two-fold: test setup information and SIP specific.

Test setup information contains:

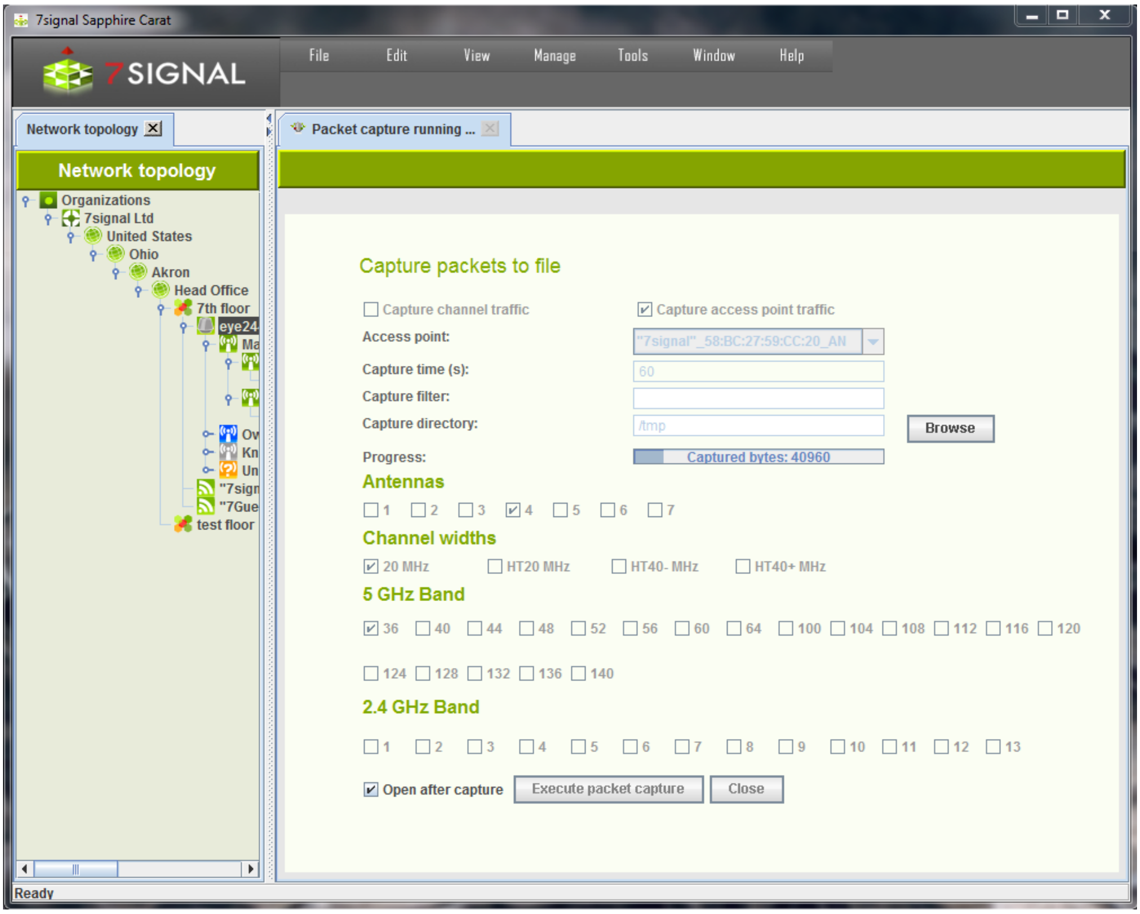
- attach time
- DHCP retrieval time
- Eye IP address used in WLAN interface
- The gateway

SIP results contain:

- used IEEE802.11e traffic category
- SIP server response for REGISTER: SIP protocol code
- Register time, milliseconds
- Authentication information (optional)
- SIP server response for UNREGISTER: SIP protocol code
- Unregister time, milliseconds

18.17 Packet capture test

Packet capture test executes packet capture on selected Eye, and resulted capture file will be downloaded to PC running the Management GUI. Packet capture can be run either for a selected access point or with selected antenna, channel and capture filter. Optionally, the downloaded capture file will be automatically opened in selected packet capture viewer (e.g. Wireshark)[40].



Capture packets to file

☐ Capture channel traffic ☑ Capture access point traffic

Access point: "7signal"_58:BC:27:59:CC:20_AN

Capture time (s): 60

Capture filter:

Capture directory: /tmp [Browse]

Progress: Captured bytes: 40960

Antennas

☐ 1 ☐ 2 ☐ 3 ☑ 4 ☐ 5 ☐ 6 ☐ 7

Channel widths

☑ 20 MHz ☐ HT20 MHz ☐ HT40- MHz ☐ HT40+ MHz

5 GHz Band

☑ 36 ☐ 40 ☐ 44 ☐ 48 ☐ 52 ☐ 56 ☐ 60 ☐ 64 ☐ 100 ☐ 104 ☐ 108 ☐ 112 ☐ 116 ☐ 120

☐ 124 ☐ 128 ☐ 132 ☐ 136 ☐ 140

2.4 GHz Band

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13

☑ Open after capture [Execute packet capture] [Close]

Figure 60: Packet capture test

1. In the Network topology, select the Eye that will run the test
2. Right-click and select “Packet capture”
3. Select capture type: “Capture channel traffic” or “Capture access point traffic”
    a. *Capture channel traffic*
        i. Select an antenna[41]
        ii. Select a channel width
        iii. Select a channel
        iv. Enter capture filter (optional)[42]
    b. *Capture access point traffic*
        i. Select access point from “Access point: “ drop-down list.
4. Enter capture time (in seconds)
5. Browse the directory to which the capture files will be downloaded.

[40] The viewer application must be configured before using this feature. Packet capture viewer application can be configured in “Edit | Configure tools” dialog.

[41] Only one antenna available in Soft and Micro Eyes

[42] Standard tcpdump capture filter format is applied.

6. Optionally, select “Open after capture” check-box.
7. Select “Execute packet capture”.
8. Capture progress can be seen in the progress bar.
9. After capture is completed, the capture file is available in the selected directory (and optionally opened with packet capture viewer)

19 SERVICE LEVEL AGREEMENT

Service Level Agreement (SLA) groups a number of KPIs and their expected target values. In a nutshell, typically a KPI has a scalar value while SLA is combination of numerous KPI values and statistical rules that result in a higher-level view on the quality of the network.

The ultimate goal is to bind together a contractual agreement and actual measurements, the expression of the desired or required level of the service and the proven real-life phenomena. As such, the SLA is a communication medium between the service provider and the customer.

The SLA outcome is percentage value and based on user-defined thresholds it is divided into values green, yellow and red according the three-basket principle. This means that the end-user experience on the WLAN network might remain adequate but the resulting SLA value is clearly in the red basket.

Related icons

SLA template	SLA KPI definition
SLA group	KPI definition

19.1 Defining a Service Level Agreement into the system

A network service provider can make Service Level Agreements (SLA) with their customers, defining the level of service provided to the customer. 7signal Sapphire enables users to monitor the fulfillment of the various performance level guarantees defined in the SLA.

> The user may freely choose the performance indicators to be monitored in the service level agreement, in effect forming out of them an SLA group.

19.2 Defining SLA Key Performance Indicators (KPI)

In 7signal Sapphire an SLA group is formed out of a set of Key Performance Indicators corresponding to the SLA. The SLA group is bound to a topology element in the monitored network. If an SLA group is not bound to a topology element, 7signal Sapphire applies the *default SLA group*, or if not defined, the SLA limits defined for KPIs in the SLA template.

An SLA group consists of several KPIs which define the boundary values used in monitoring the fulfillment of the service level agreement.

In the 7signal Sapphire system the boundary values can be set separately for each KPI contained in the SLA group. Each KPI defines a certain type of boundary value and percentage values for how many measurement samples may fall outside the defined boundary values without causing the service level agreement to be considered unfulfilled. The type of the KPI determines whether measurement samples with values over or under the boundary value are desired.

Three color coding is used for service levels in the KPIs: green, yellow and red. The percentage boundaries are defined for green and yellow levels of service.

To attain the green level of service the percentage of measurement samples that fulfill the boundary value criteria set in the KPI (that is, are over or under the set boundary value, depending on the type of KPI) must be at least as high as the percentage boundary value set for the green level in the KPI. If there are too many measurement samples that do not fulfill the boundary value criteria, the service level falls to yellow. The yellow level functions likewise: if it is not attained, the service level falls to red.

As an example, the table below explains how an SLA value is calculated for Upload Throughput KPI, its measurement and statistical analysis.

Boundary value	above 5,5 Mbit/s	The threshold value for KPI.
Green level	99,0%	At least 99,0% of measured samples must attain an upload throughput of at least 5,5Mbit/s in order to attain the green level for the KPI in question.
Yellow level	95,0%	If the percentage of measured samples that satisfy the boundary value criteria falls between 95,0% and 99% the yellow level is attained.
Red level	below 95,0%	If the percentage falls below 95,0% the service level can be considered unfulfilled.

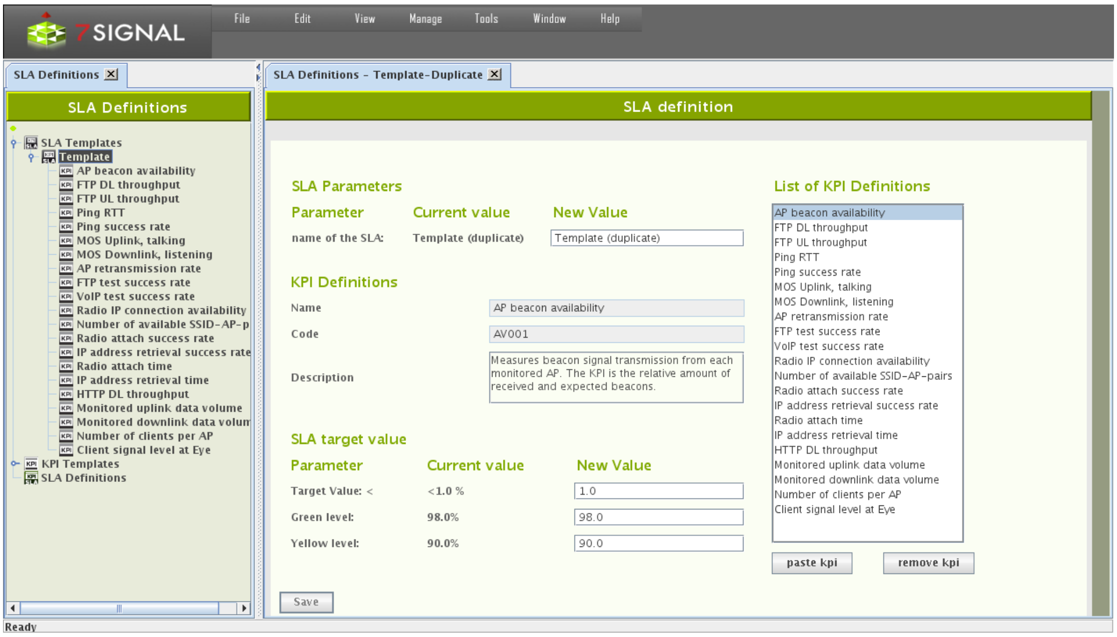
19.3 Creating an SLA group

An SLA group can be created in one of two ways:

1. By copying an SLA template
2. By creating an empty SLA group and adding to it the desired Key Performance Indicators

When the desired set of KPIs has been added to the SLA group the KPI boundary values can be set to match the service levels outlined in the actual Service Level Agreement contract.

19.3.1 Creating an SLA group from a template



SLA Parameters

Parameter	Current value	New Value
name of the SLA:	Template (duplicate)	Template (duplicate)

KPI Definitions

Name: AP beacon availability

Code: AV001

Description: Measures beacon signal transmission from each monitored AP. The KPI is the relative amount of received and expected beacons.

SLA target value

Parameter	Current value	New Value
Target Value: <	<1.0 %	1.0
Green level:	98.0%	98.0
Yellow level:	90.0%	90.0

Figure 61: Creating SLA group from a template

Create the SLA group as follows:

1. Click on "Manage | SLA definitions" from the top menu bar
2. Open Templates node.

3. Right-click on the desired SLA template
4. Choose "Duplicate" from the pop-up menu. An SLA group editing dialog opens to the right (pictured above)
5. Name the SLA group
6. Remove unnecessary KPIs from the "KPI definitions" list by using the "Remove KPI" button
7. Add wanted KPI's which are not within the template. See next chapter how to do this.
8. If it's desired to change the boundary values of KPIs, choose the desired KPI from the "KPI definitions" list. The KPI's name, description and boundary values according to service level agreement are updated into the editing dialog.
9. Edit the boundary values to your liking.
10. Repeat from step 7. until every boundary value is as desired.
11. Click "Save"

19.3.2 Creating an SLA group from scratch

The dialog pane is identical to the case of duplicated template. Naturally the contents of the pane are empty, but the look and the process are identical.

Create the SLA group as follows:

1. Click on "Manage | SLA definitions" from the top menu bar
2. Right-click on "SLA groups" from the tree hierarchy
3. Choose "Add SLA group" from pop-up menu. An SLA group editing dialog opens to the right.
4. Name the SLA group
5. Choose "KPI definitions" from the tree hierarchy. Available KPIs are opened into the tree.
6. Right-click on the desired KPI
7. Choose "Copy" from the pop-up menu
8. Click "Paste KPI" from the SLA group editing dialog
9. Choose the KPI in the SLA group editing dialog ("KPI definitions"). The KPI's name, description and boundary values according to service level agreement are updated into the editing dialog.
10. If necessary, edit the boundary values.
11. Repeat from step 6. onwards until all desired KPIs have been added to the SLA group.
12. Click "Save"

19.3.3 Setting default SLA group

An SLA group can be defined as the *default SLA group*. The default SLA group is applied if no other SLA group is effective on topology elements.

Set an SLA group as the default SLA group as follows:

1. Click on "Manage | SLA definitions" from the top menu bar
2. Open “SLA Definitions” node.
3. Right-click on the desired SLA group
4. Choose "Set as default group" from the pop-up menu. Suffix “(default)” will appear from the end of the SLA group name in the tree.

There can be only one default SLA group. In order to change the default SLA group, or completely remove use of default SLA group feature, the current default SLA group must be changed to ordinary SLA group:

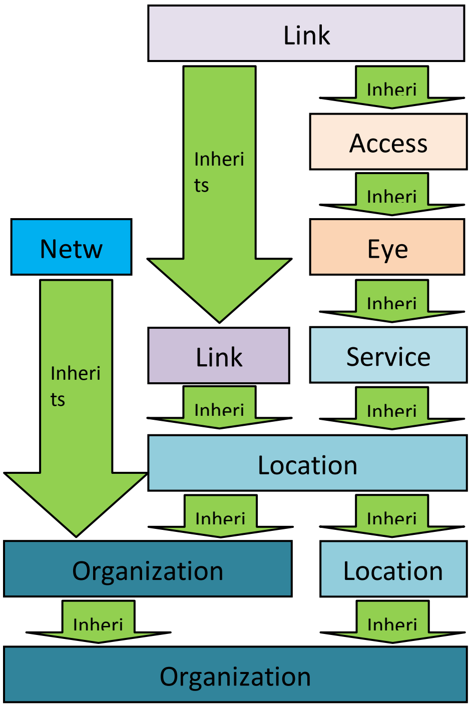
1. Click on "Manage | SLA definitions" from the top menu bar
2. Open “SLA Definitions” node.
3. Right-click on the desired SLA group
4. Choose "Set as not default group" from the pop-up menu. Suffix “(default)” will disappear from the end of the SLA group name in the tree.

19.4 SLA propagation

An SLA Group can be bound to any topology element type. In order to avoid unnecessary binding of the same SLA Groups to multiple topology elements, there is a propagation hierarchy how SLA Groups are propagated from different levels within the topology hierarchy.

This means that for example if SLA Group is only bound to Top level organization, it is propagated to each element under the organization. On the other hand, if an SLA Group is explicitly bound to a topology element, this SLA Group is always applied to the topology element.

The following figure depicts the SLA propagation order:



Propagation rules are the following:

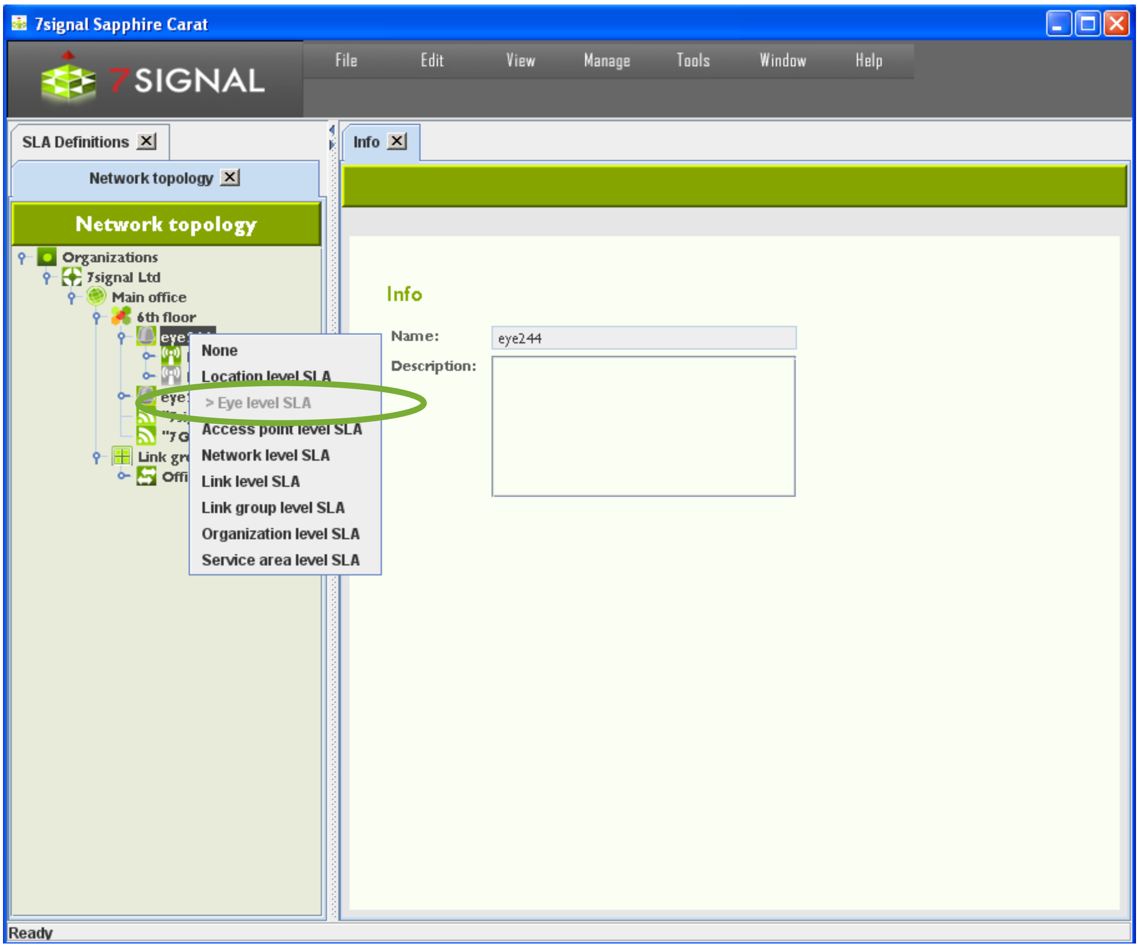
- Wireless network inherits from Organization.
  - If the Organization does not have a bound SLA Group, Wireless network inherits SLA Group from parent Organization of its own Organization.
- Link inherits from Access Point or Link Group.
  - If both have an SLA Group, SLA Group is inherited from the Access Point.
  - If the Access Point does not have a bound SLA Group, the Link inherits the Group from Eye, etc.
  - If the Link Group does not have a bound SLA Group, the Link inherits the Group from the Location, etc.

- Link Group inherits from Location.
  - If the Location does not have a bound SLA Group, the Link Group inherits from parent Location or Organization, etc.
- Access Point inherits from Eye.
  - If the Eye does not have a bound SLA Group, the Access Point inherits from Service Area, etc.
- Eye inherits from Service Area.
  - If the Service Area does not have a bound SLA Group, the Service Area inherits from Location, etc.
- Service Area inherits from Location.
  - If the Location does not have a bound SLA Group, the Service Area inherits from parent Location or Organization, etc.
- Location inherits from parent Location or Organization.
  - If the parent Location or Organization does not have a bound SLA Group, the Location inherits from parent Location or Organization, etc.
- Organization inherits from parent Organization.

Management GUI shows the bound or inherited SLA group:

1. In Network Topology select a topology element
2. Right-click and select “Bind SLA”

If the SLA Group is explicitly bound to the topology element, the bound SLA Group can be seen in the selected state:

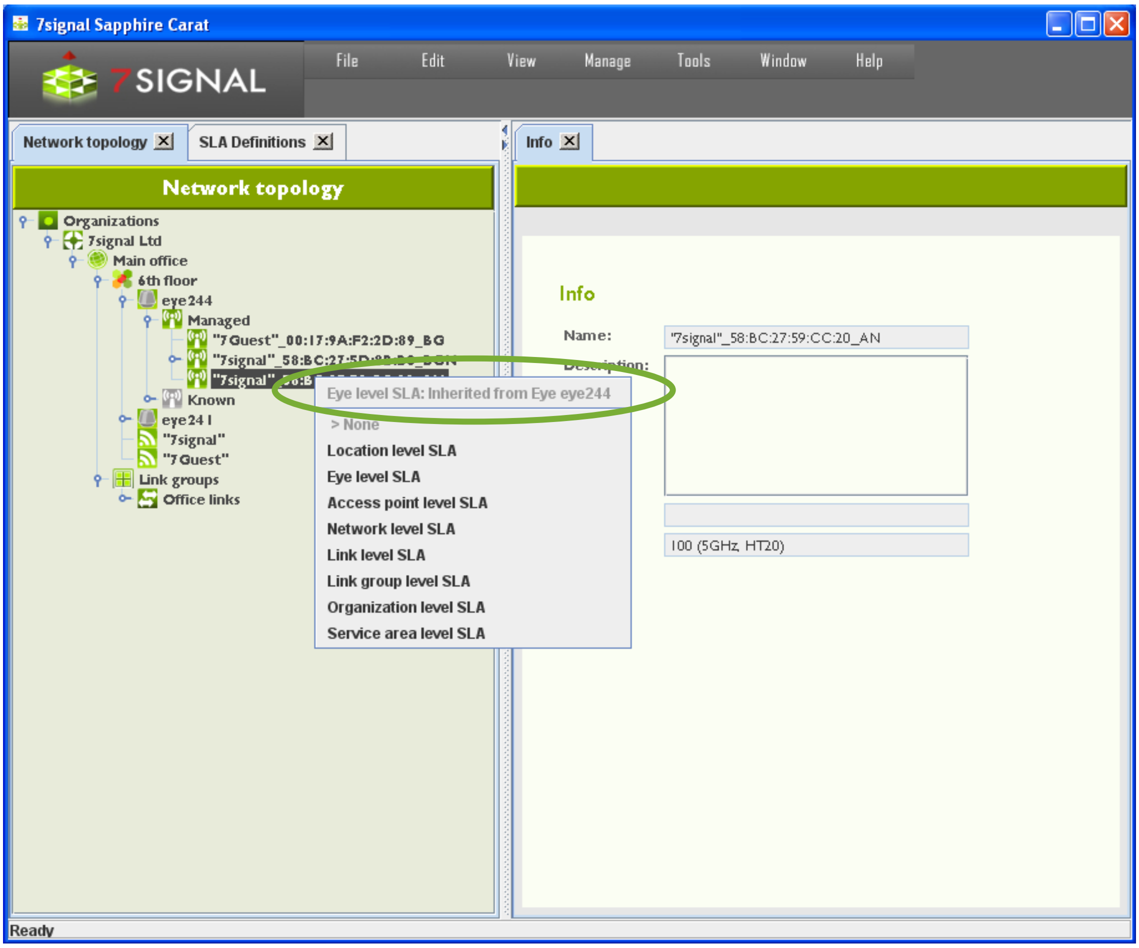


Name: eye244

Description:

Figure 62: SLA Group bound to an Eye

If the SLA Group is inherited, the name of the SLA Group and the name topology element from which the SLA Group is inherited is shown:



Name: "7signal"_58:BC:27:59:CC:20_AN

Description:

100 (5GHz, HT20)

Figure 63: SLA Group inherited from SLA Group bound to an Eye

19.5 Binding SLA Groups

19.5.1 Binding an SLA group to a Link

Bind an SLA group to a link as follows:

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the link that you want to bind an SLA group to from the tree hierarchy
3. Choose "Set SLA group" from the pop-up menu
4. Choose the desired SLA group from the menu that opens

Or alternatively

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the link that you want to bind an SLA group to from the tree hierarchy
3. Select "Edit" from the pop-up menu. A link editing dialog opens to the right
4. Choose the desired SLA group from the drop-down menu
5. Click "Save"

19.5.2 Binding an SLA group to a link group

Bind an SLA group to a link group as follows:

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the link group that you want to bind an SLA group to from the tree hierarchy
3. Choose "Set SLA group" from the pop-up menu
4. Choose the desired SLA group from the menu that opens

Or alternatively

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the link group that you want to bind an SLA group to from the tree hierarchy
3. Select "Edit" from the pop-up menu. A link group editing dialog opens to the right
4. Choose the desired SLA group from the drop-down menu
5. Click "Save"

19.5.3 Binding an SLA Group to other Entities

SLA Group can be bound to any entity within the Topology Tree. This can be done as follows

1. Right click the topology element and select “Bind SLA”
2. Select the SLA from the given list.

20 CONTINUOS AND AUTOMATED REPORTING

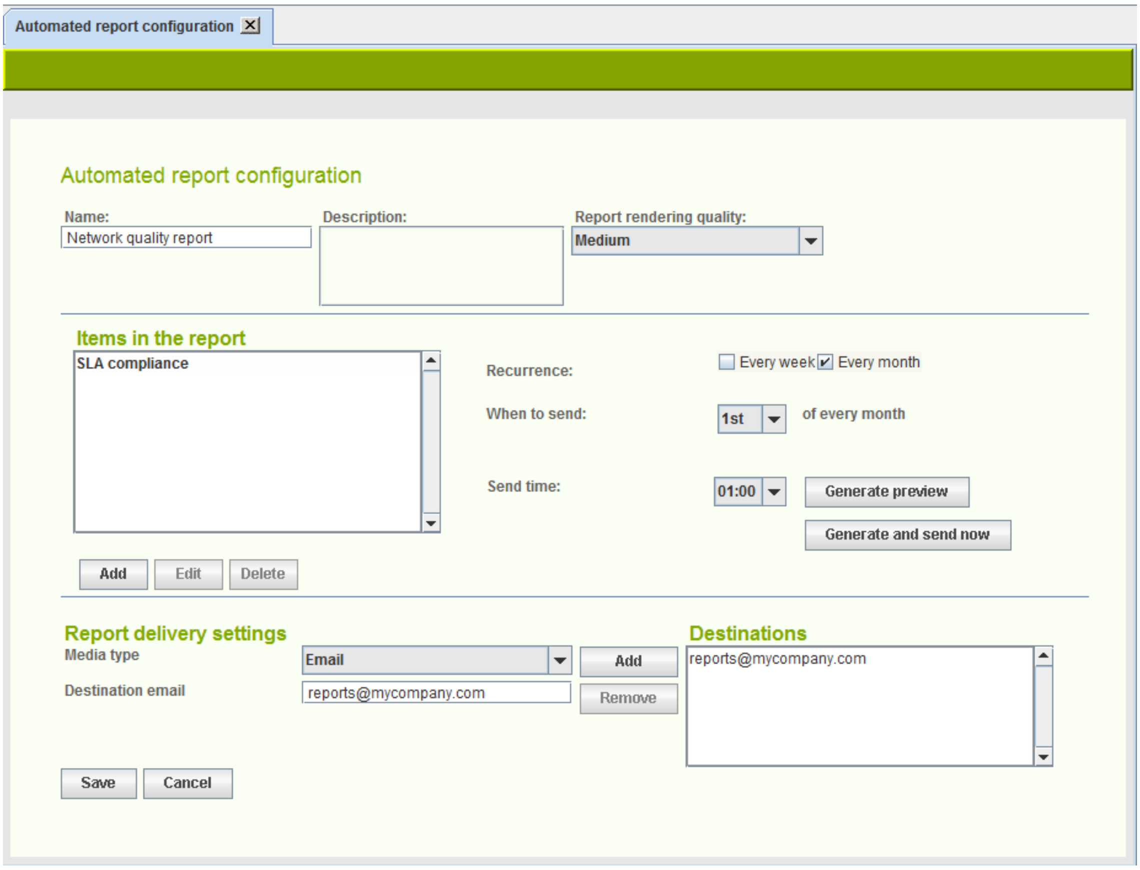
Analyzer is an interactive tool for studying network phenomena of interest and for in-depth investigation of problems. Reports in standard, easy-to-interpret formats are available to support routine monitoring.

By using the report view in Carat, the user can configure reports from elements that are familiar from Analyzer. In addition to the user-selected indicators, a report configured here contains the time of compilation and delivery and a list of the delivery addresses. At the specified time, Carat generates the report and delivers it to the recipients, specified as either e-mail addresses or directories in the Carat server file system. A report can include KPIs, service level views, and alarms, referred to below as report items.

> Note: Configuring the mail server settings found under "Edit | SMTP server" enables the use of email in reporting.

20.1 Subscription for a new report

1. Select "Manage | Automated report configuration"
2. Select "New" to create a new subscription and open a report template
   a. Use "Edit" for editing a subscription
   b. The "Delete" option allows you to delete a subscription
   c. When you select a report name, the description of this existing report is displayed



Automated report configuration

Name: Network quality report

Description:

Report rendering quality: Medium

Items in the report

SLA compliance

Recurrence: □ Every week ☑ Every month

When to send: 1st of every month

Send time: 01:00

Report delivery settings

Media type: Email

Destination email: reports@mycompany.com

Destinations

reports@mycompany.com

Figure 64: Automated report configuration

In the "Report Properties Configuration" area:

3. Enter a name for the subscription
4. Enter a description for the subscription (optional)
5. Select an report image (optional)
6. Choose the location for the image on the page
   The image will be repeated on each page of the report. It might represent, for example, a company or a target network.
7. Select the resolution (quality) to be used for the report graphics, mainly relevant to charting.

In the “Report items” area:

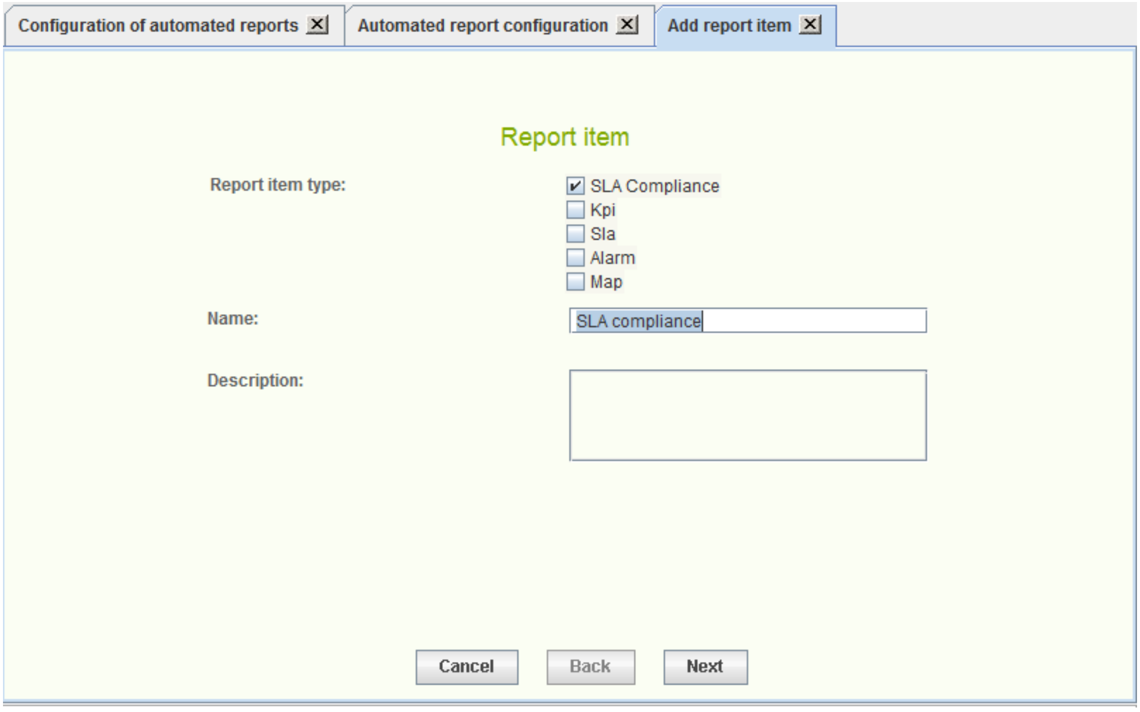
8. Configure the items to be included in the report by selecting “Add”
   a. this starts content-dependent workflows, instructions below
9. Specify the send time
   a. recurrence is weekly or monthly
      i. Field “When to send” is dynamic and let’s one choose either numerous week days or a day in month
   b. send time has 30 minutes resolution in a drop-down menu
10. “Generate preview” creates a report and opens it is a viewer tool
11. “Generate and send now” are available for subscriptions that have been saved (report will be generated and sent to recipients, see “Report destination settings”).

In the “Report destination settings” area:

12. Choose the delivery format (**Media type**) of the PDF report
    a. Email
    b. save to **File** system
       i. an absolute path gives the location in the Carat server file system
       ii. relative paths are relative to the Carat startup directory (default: /opt/7signal/Carat/7signal)
13. Add one or more formats in the “Destinations” field by clicking “Add”
14. Save the subscription by clicking “Save”

20.2 Adding Report Items

There are five report item types. A report item is an individual piece of information – SLA compliance, a KPI chart, an SLA table, a map, or a set of alarms – that is part of the report. A report is a series of report items.


Configuration of automated reports
Automated report configuration
Add report item
Report item

Report item type:
☑ SLA Compliance
□ Kpi
□ Sla
□ Alarm
□ Map

Name: SLA compliance

Description:

Figure 65: Adding a report item

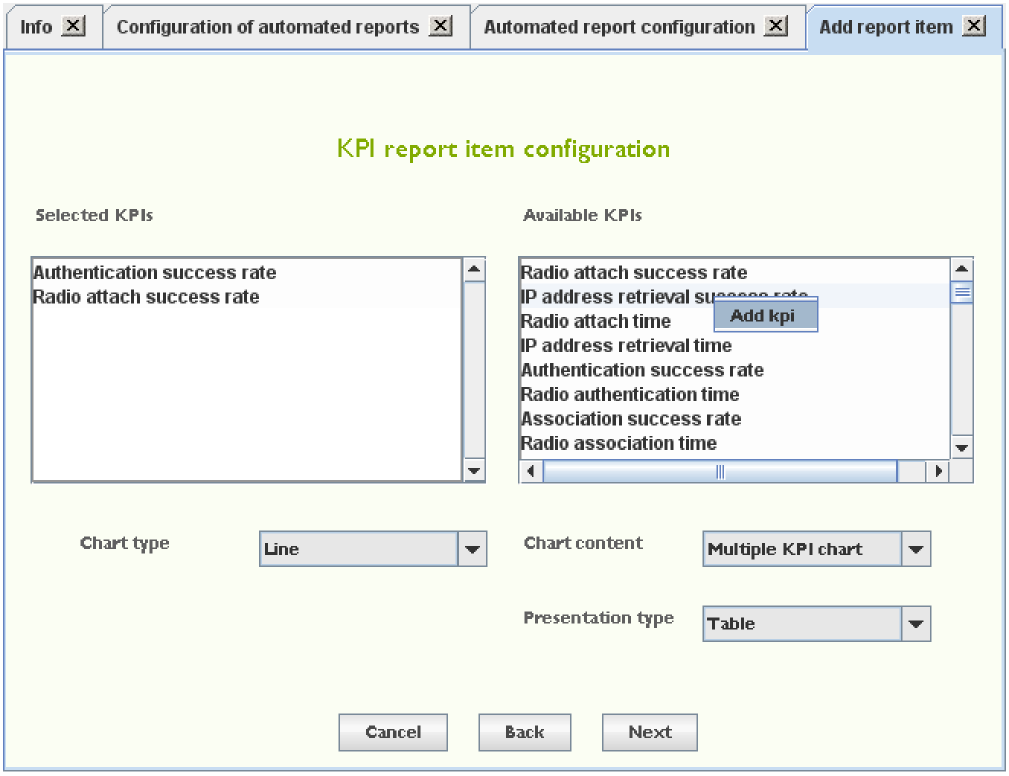
To add a report item:

1. Choose the content type
2. Give a name to the report item
    a. a descriptive name is good especially if the item content groups together numerous pieces of information
3. Optionally write a description of the report item
4. Select “Next”

20.2.1 Adding SLA compliance report item

1. Select topology elements of the report item. See chapter 20.2.6.
2. Click “Next” to continue to “Report item time configuration”. See chapter 20.2.6.

20.2.2 Adding KPI report item


Info
Configuration of automated reports
Automated report configuration
Add report item
KPI report item configuration
Add kpi
Cancel
Back
Next

Selected KPIs

Authentication success rate
Radio attach success rate

Available KPIs

Radio attach success rate
IP address retrieval su
Radio attach time
IP address retrieval time
Authentication success rate
Radio authentication time
Association success rate
Radio association time

Chart type: Line

Chart content: Multiple KPI chart

Presentation type: Table

Figure 66: Multiple KPI chart report item

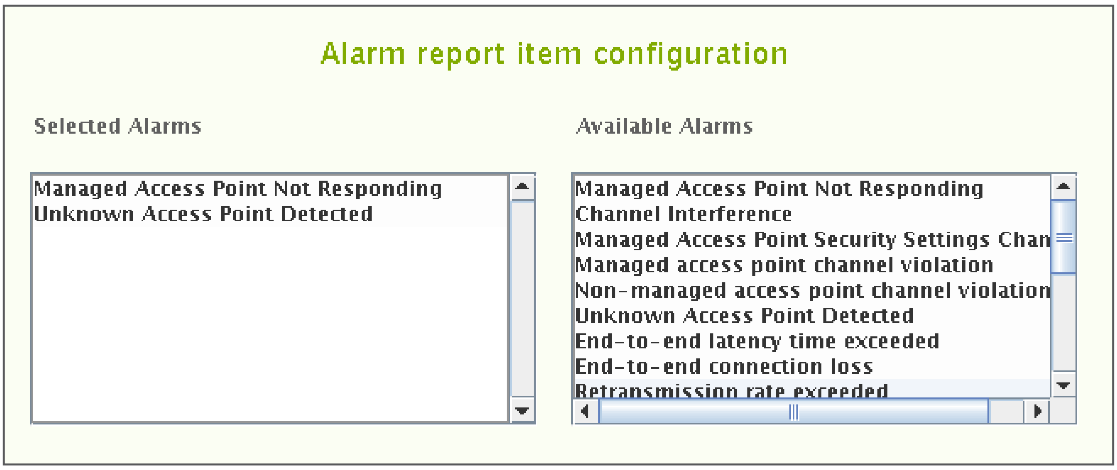
3. Select the desired KPI by left-clicking it in the right-hand pane
4. Right-click and select “Add KPI” in the submenu
5. Repeat steps 2–3 until all desired KPIs are in the left pane (depending on chart type: “Multiple KPI chart allows more than one KPI)
6. Select the **Chart type**
7. Select the method for displaying the measurement series in **Chart content**
8. Select the display method
    a. Data **Table**, Aggregation **Chart**
9. Click “Next” to continue to “Report item topology configuration”. See chapter 20.2.6.
10. Click “Next” to continue to “Report item time configuration”. See chapter 20.2.6.

20.2.3 Adding SLA report item

.

1. Choose the topology elements of the report item. See chapter 20.2.6.
2. Click “Next” to continue to “Report item time configuration”. See chapter 20.2.6.

20.2.4 Adding alarm report item



Alarm report item configuration

Selected Alarms

Managed Access Point Not Responding
Unknown Access Point Detected

Available Alarms

Managed Access Point Not Responding
Channel Interference
Managed Access Point Security Settings Chan
Managed access point channel violation
Non-managed access point channel violation
Unknown Access Point Detected
End-to-end latency time exceeded
End-to-end connection loss
Retransmission rate exceeded

Figure 67: Adding alarm report item

1. Select the desired alarm by left-clicking it in the right-hand pane
2. Right-click the alarm and select “Add alarm” in the submenu
    a. One may remind oneself about the alarm by selecting “Description”
3. Repeat steps 2–3 until all of the desired alarms are in the left pane
4. Select “Next” to continue to “Report item topology configuration”. See chapter 20.2.6.
5. Select the time interval for the report. See chapter 20.2.6.

20.2.5 Adding map report item

1. Select the desired KPI by left-clicking it in the right-hand pane
2. Right-click and select “Add KPI” in the submenu
3. Click “Next” to continue to “Report item topology configuration”. See chapter 20.2.6.
4. Click “Next” to continue to “Report item time configuration”. See chapter 20.2.6.

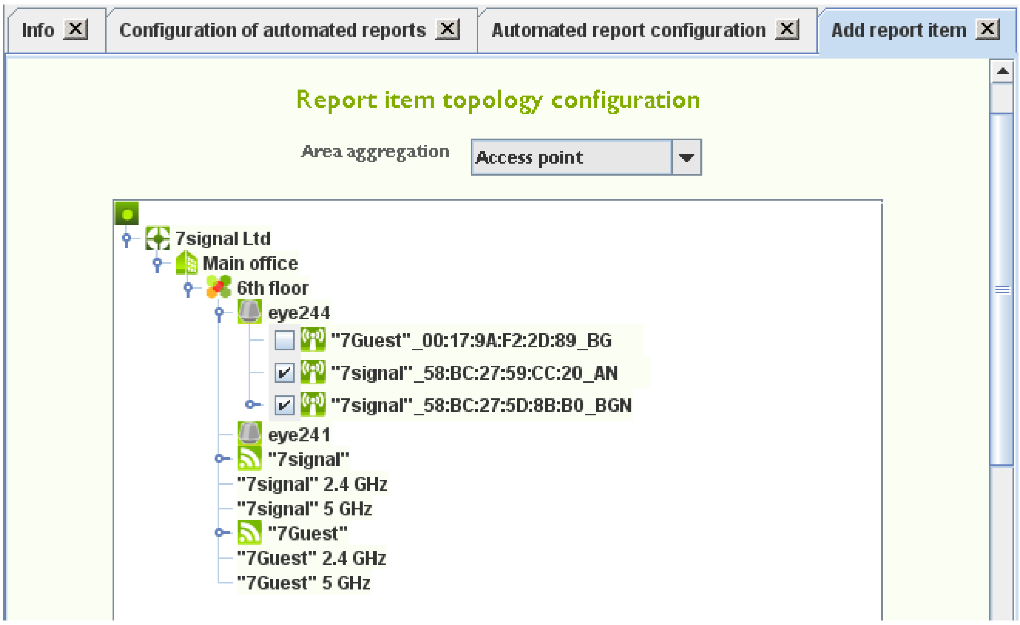
20.2.6 Report item general options

All report item types have two configuration options: report item topology configuration and report item time configuration. The general configuration options are asked after report item specific options.

Report item topology configuration

The report item time configuration dialog contains two elements:

- Area aggregation selector
- Topology tree


Info
Configuration of automated reports
Automated report configuration
Add report item

Report item topology configuration

Area aggregation: Access point

- 7signal Ltd
  - Main office
    - 6th floor
      - eye244
        - □ "7Guest"_00:17:9A:F2:2D:89_BG
        - ☑ "7signal"_58:BC:27:59:CC:20_AN
        - ☑ "7signal"_58:BC:27:5D:8B:B0_BGN
      - eye241
      - "7signal"
      - "7signal" 2.4 GHz
      - "7signal" 5 GHz
      - "7Guest"
      - "7Guest" 2.4 GHz
      - "7Guest" 5 GHz

Figure 68: Report item topology configuration, access point area aggregation

Available area aggregations[43] depend on report item type:

Table 13: Supported area aggregations

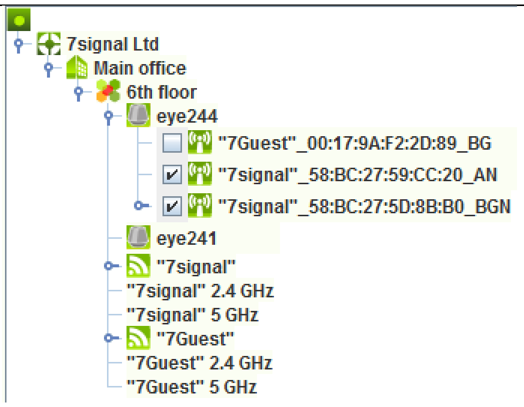
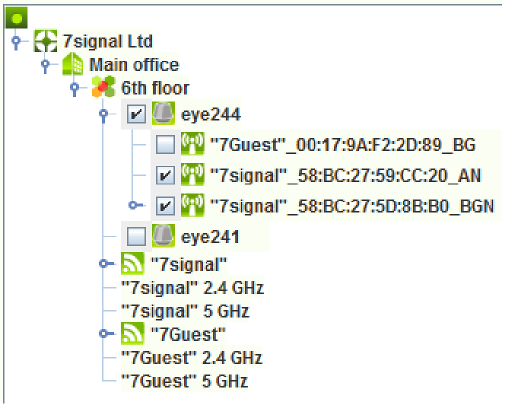
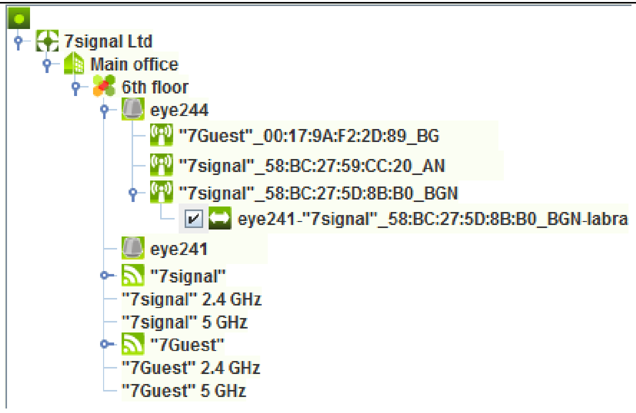
Report item type	Supported area aggregations
SLA compliance	Access point Network Link
KPI	Network Access point APEye Link NWServ NWBandServ NWEye NWBand NWBandEye Dest DestAP DestEye DestEyeEth EyeEth
SLA	Network Access point APEye Link NWServ NWBandServ NWEye NWBand NWBandEye Dest DestAP DestEye DestEyeEth EyeEth
Alarm	Access point

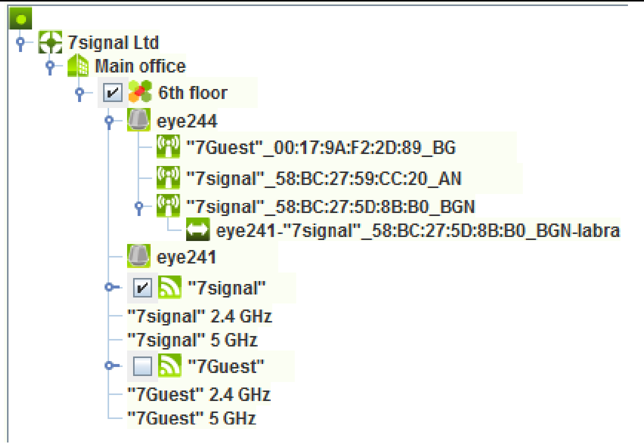
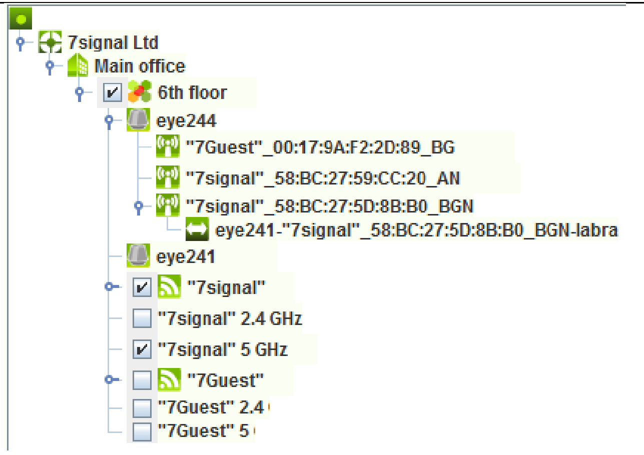
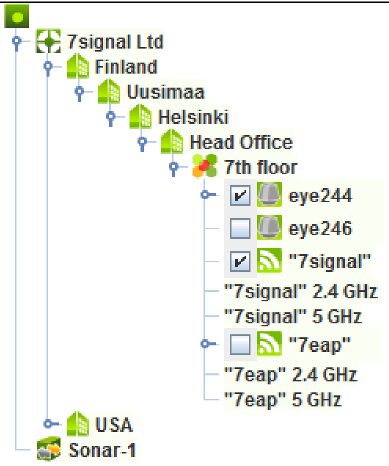
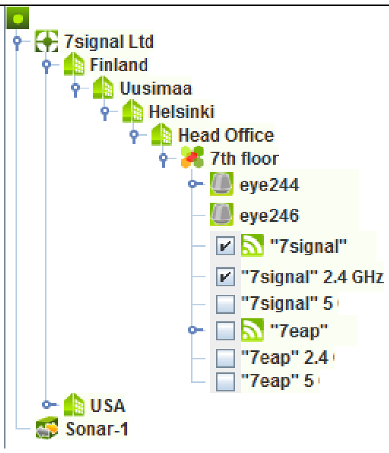
[43] For more about area aggregations, please see Analyzer User Manual.

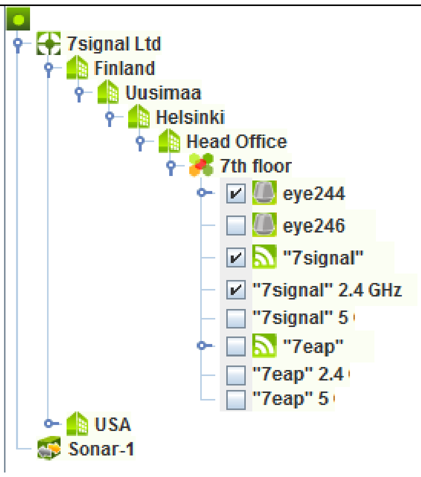
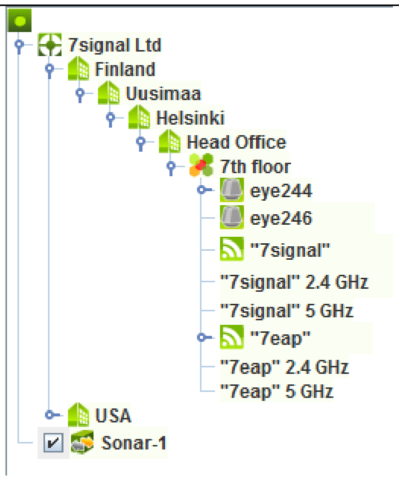
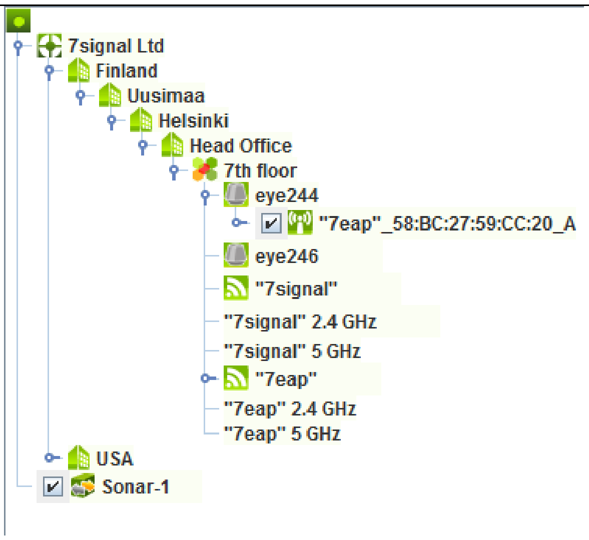
Map	Serv NWBandServ

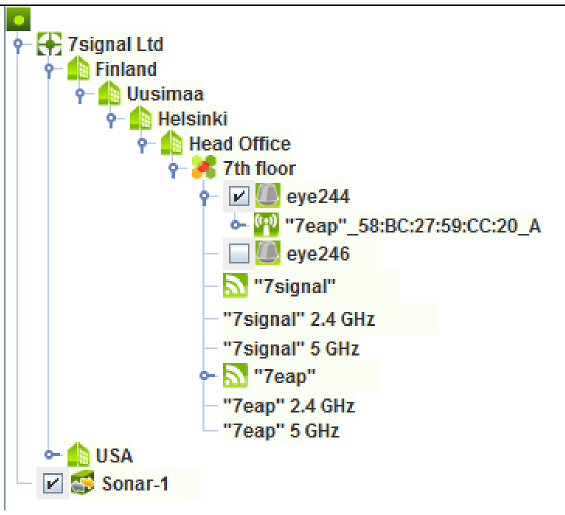
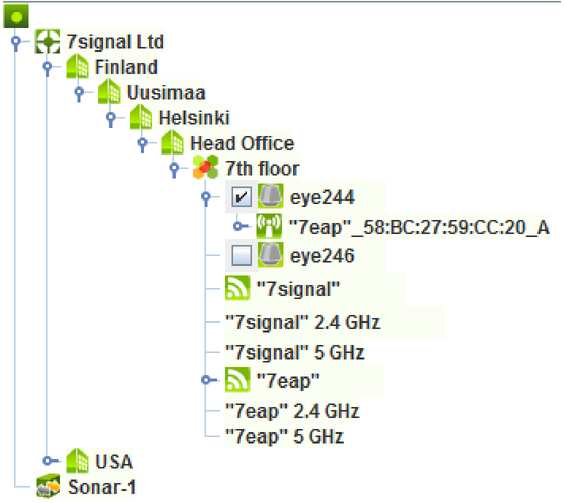
Topology tree is used for selecting topology elements to the report item. Which topology elements can be selected depends on the chosen area aggregation. Notice that on Map report items, there must be a map configured for the Service Area.

Table 14: Report item topology element selections per area aggregation

Area aggregation	Topology elements	Example
Access point	At least one access point	 7signal Ltd Main office 6th floor eye244 ☐ "7Guest"_00:17:9A:F2:2D:89_BG ☑ "7signal"_58:BC:27:59:CC:20_AN ☑ "7signal"_58:BC:27:5D:8B:B0_BGN eye241 "7signal" "7signal" 2.4 GHz "7signal" 5 GHz "7Guest" "7Guest" 2.4 GHz "7Guest" 5 GHz
APEye	At least one Eye and access point managed by the Eye	 7signal Ltd Main office 6th floor ☑ eye244 ☐ "7Guest"_00:17:9A:F2:2D:89_BG ☑ "7signal"_58:BC:27:59:CC:20_AN ☑ "7signal"_58:BC:27:5D:8B:B0_BGN ☐ eye241 "7signal" "7signal" 2.4 GHz "7signal" 5 GHz "7Guest" "7Guest" 2.4 GHz "7Guest" 5 GHz
Link	At least one Link	 7signal Ltd Main office 6th floor eye244 "7Guest"_00:17:9A:F2:2D:89_BG "7signal"_58:BC:27:59:CC:20_AN "7signal"_58:BC:27:5D:8B:B0_BGN ☑ eye241-"7signal"_58:BC:27:5D:8B:B0_BGN-labra eye241 "7signal" "7signal" 2.4 GHz "7signal" 5 GHz "7Guest" "7Guest" 2.4 GHz "7Guest" 5 GHz

NWServ	At least one Service Area and Network	 7signal Ltd Main office ☑ 6th floor eye244 "7Guest"_00:17:9A:F2:2D:89_BG "7signal"_58:BC:27:59:CC:20_AN "7signal"_58:BC:27:5D:8B:B0_BGN eye241-"7signal"_58:BC:27:5D:8B:B0_BGN-labra eye241 ☑ "7signal" "7signal" 2.4 GHz "7signal" 5 GHz □ "7Guest" "7Guest" 2.4 GHz "7Guest" 5 GHz
NWBandServ	At least one Service Area, Network and band of the Network	 7signal Ltd Main office ☑ 6th floor eye244 "7Guest"_00:17:9A:F2:2D:89_BG "7signal"_58:BC:27:59:CC:20_AN "7signal"_58:BC:27:5D:8B:B0_BGN eye241-"7signal"_58:BC:27:5D:8B:B0_BGN-labra eye241 ☑ "7signal" □ "7signal" 2.4 GHz ☑ "7signal" 5 GHz □ "7Guest" □ "7Guest" 2.4 □ "7Guest" 5
NWEye	At least one Network and Eye	 7signal Ltd Finland Uusimaa Helsinki Head Office 7th floor ☑ eye244 □ eye246 ☑ "7signal" "7signal" 2.4 GHz "7signal" 5 GHz □ "7eap" "7eap" 2.4 GHz "7eap" 5 GHz USA Sonar-1
NWBand	At least one Network and band of the Network	 7signal Ltd Finland Uusimaa Helsinki Head Office 7th floor eye244 eye246 ☑ "7signal" ☑ "7signal" 2.4 GHz □ "7signal" 5 □ "7eap" □ "7eap" 2.4 □ "7eap" 5 USA Sonar-1

NWBandEye	At least one Network, band of the Network and Eye	 7signal Ltd Finland Uusimaa Helsinki Head Office 7th floor ☑ eye244 ☐ eye246 ☑ "7signal" ☑ "7signal" 2.4 GHz ☐ "7signal" 5 ☐ "7eap" ☐ "7eap" 2.4 ☐ "7eap" 5 USA Sonar-1
Dest	At least one Sonar	 7signal Ltd Finland Uusimaa Helsinki Head Office 7th floor eye244 eye246 "7signal" "7signal" 2.4 GHz "7signal" 5 GHz "7eap" "7eap" 2.4 GHz "7eap" 5 GHz USA ☑ Sonar-1
DestAP	At least one Sonar and Access Point	 7signal Ltd Finland Uusimaa Helsinki Head Office 7th floor eye244 ☑ "7eap"_58:BC:27:59:CC:20_A eye246 "7signal" "7signal" 2.4 GHz "7signal" 5 GHz "7eap" "7eap" 2.4 GHz "7eap" 5 GHz USA ☑ Sonar-1

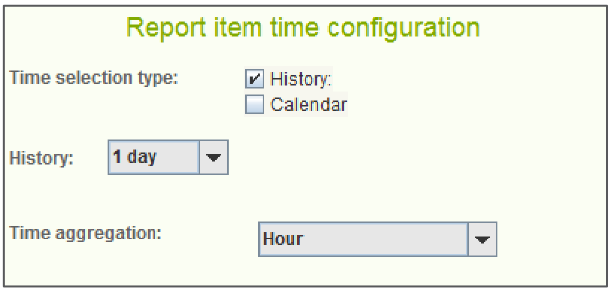
DestEye DestEyeEth	At least one Sonar and Eye	 7signal Ltd Finland Uusimaa Helsinki Head Office 7th floor ☑ eye244 "7eap"_58:BC:27:59:CC:20_A ☐ eye246 "7signal" "7signal" 2.4 GHz "7signal" 5 GHz "7eap" "7eap" 2.4 GHz "7eap" 5 GHz USA ☑ Sonar-1
EyeEth	At least one Eye	 7signal Ltd Finland Uusimaa Helsinki Head Office 7th floor ☑ eye244 "7eap"_58:BC:27:59:CC:20_A ☐ eye246 "7signal" "7signal" 2.4 GHz "7signal" 5 GHz "7eap" "7eap" 2.4 GHz "7eap" 5 GHz USA Sonar-1

Steps for report item topology configuration:

1. Select the **Area aggregation**
2. From the hierarchical tree presented, select the corresponding elements depending on the selected area aggregation.
3. Click “Next” to continue to “Report item time configuration”

Report item time configuration

Report time configuration dialog contains time interval and time aggregation selectors.



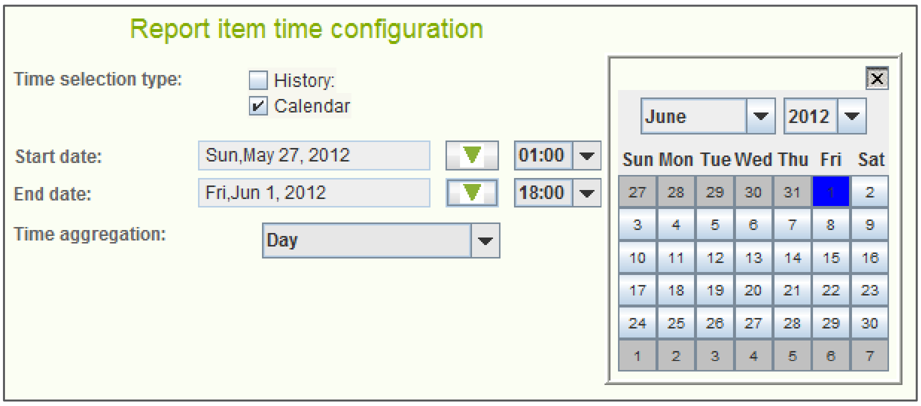
Report item time configuration

Time selection type: ☑ History: ☐ Calendar

History: 1 day

Time aggregation: Hour

Figure 69: Report item time configuration, history mode



Report item time configuration

Time selection type: □ History: ☑ Calendar

Start date: Sun,May 27, 2012 01:00

End date: Fri,Jun 1, 2012 18:00

Time aggregation: Day

June 2012

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Figure 70: Report time configuration, calendar mode

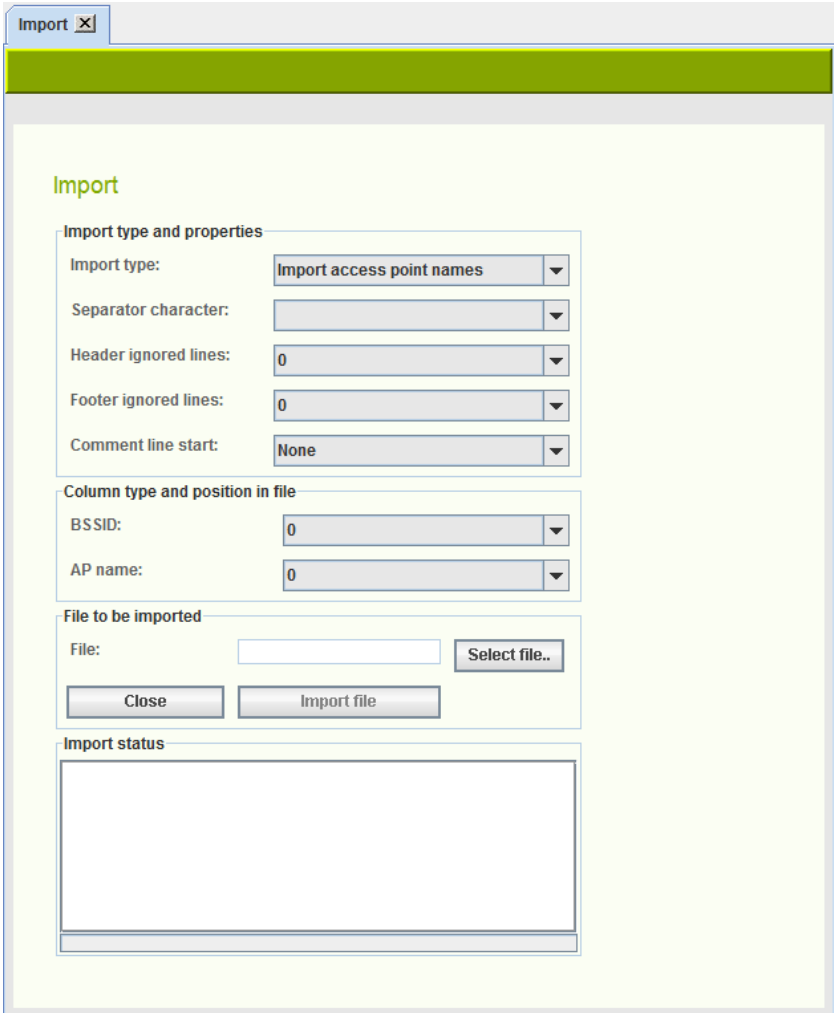
1. Select the time interval for the report
   a. **History** (in the picture above)uses pre-defined intervals from the generation time backwards
   b. **Calendar** allows free interval definition
2. Time aggregation defines the averaging period for the report item
3. Click “Finish” to return to first subscription page

21 IMPORT

Import utility supports currently importing of

- access point names
- access point names when last MAC digit is zero
- access points by replacing existing access points in the configuration

In order to import start import utility, select “Tools | Import …” from the menu. The import dialog is opened:



Import

Import type and properties

Import type: Import access point names

Separator character:

Header ignored lines: 0

Footer ignored lines: 0

Comment line start: None

Column type and position in file

BSSID: 0

AP name: 0

File to be imported

File:

Import status

Figure 71: Import dialog, access point name import selected

Select “Import type” from drop-down menu.

21.1 Importing access point names

1. Select a separator character according to field separator character in the file to be imported.
2. If the file contains header lines that should be ignored, select correct number of lines in “Header ignored lines” drop-down menu.

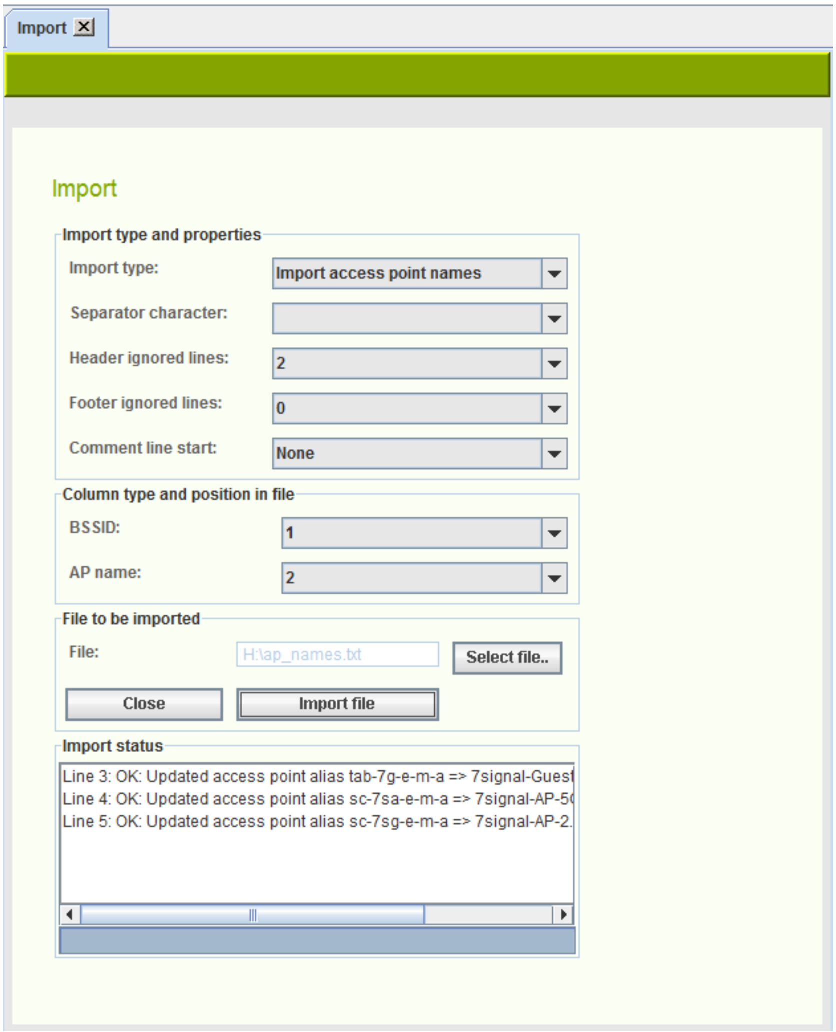
3. If the file contains footer lines that should be ignored, select correct number of lines in "Footer ignored lines" drop-down menu.
4. If the file contains comment lines that start with a specific character, select a comment line start character in "Comment line start" drop-down menu.
5. Select the BSSID column number in the file. "0" means first column, "1" means second column, etc.
6. Select the AP name column number in the file. "0" means first column, "1" means second column, etc.
7. Select the file to be imported by clicking "Select file.." button.
8. Select "Import file".
9. Check status of the import in "Import status" field.

21.1.1 Example access point name import

`ap_names.txt` file contains the following BSSID-to-name mappings:

```
SSID            MAC address              Alias

----            -----------              -----

7Guest          00:17:9A:F2:2D:89        7signal-Guest-AP

7signal         58:BC:27:59:CC:20        7signal-AP-5GHz

7signal         58:BC:27:5D:8B:B0        7signal-AP-2.4GHz
```

The file import settings and result looks like the following:



Import ☒

Import

Import type and properties

Import type: Import access point names

Separator character:

Header ignored lines: 2

Footer ignored lines: 0

Comment line start: None

Column type and position in file

BSSID: 1

AP name: 2

File to be imported

File: H:\ap_names.txt

Import status

```
Line 3: OK: Updated access point alias tab-7g-e-m-a => 7signal-Guest
Line 4: OK: Updated access point alias sc-7sa-e-m-a => 7signal-AP-5(
Line 5: OK: Updated access point alias sc-7sg-e-m-a => 7signal-AP-2.
```

- Separator character is “white space”
- Two header lines must be ignored
- No ignored lines at the end of the file
- No comment lines
- MAC address is at the second column of the file
- AP name is at the third column of the file

“Import status” field indicates that all lines were successfully imported.

21.2 Importing access point names (“last digit zero” mode)

21.2.1 Overview

This import mode is useful for importing access point names to the system from e.g. Cisco controller output. The last digit of a Cisco access point MAC address is zero, last digit of BSSIDs of the access point are non-zero.

For example:

Access point MAC address: 58:BC:27:5D:8B:B0

MAC address of first BSSID: 58:BC:27:5D:8B:B1

MAC address of second BSSID: 58:BC:27:5D:8B:B1

MAC address of third BSSID: 58:BC:27:5D:8B:B2

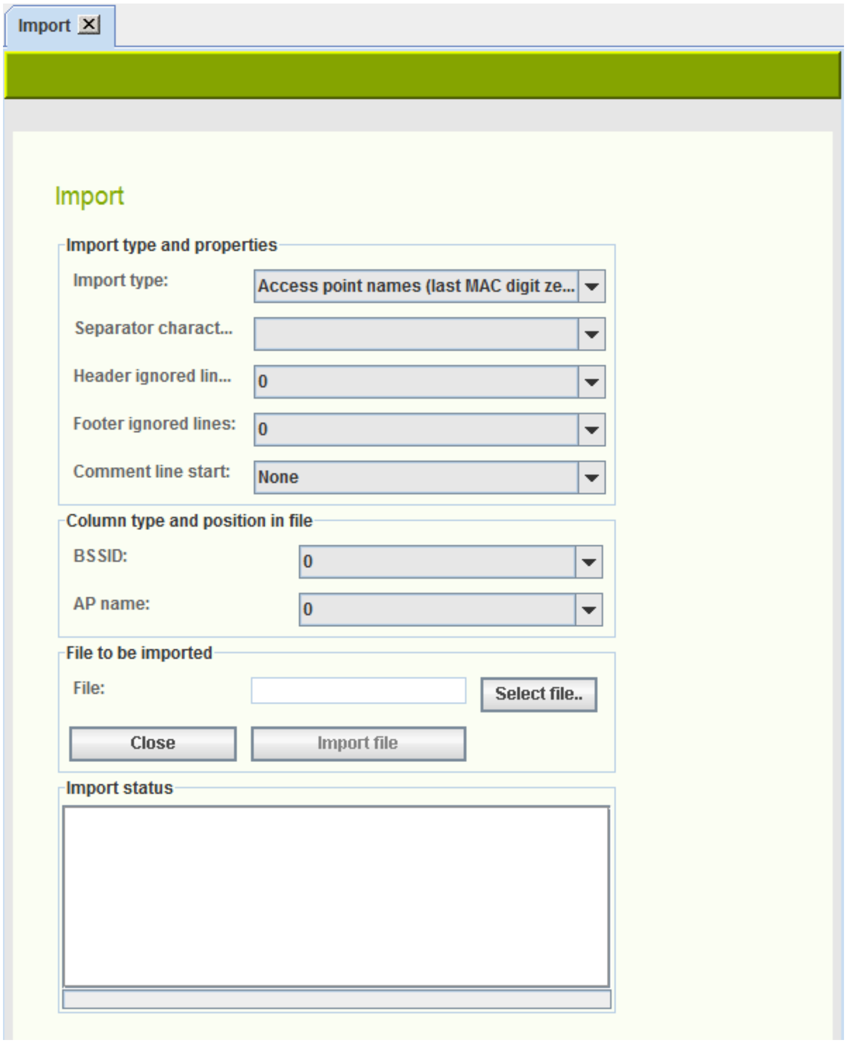
Access point name list exported from WLAN controller lists the access point names and their MAC addresses:

Test-AP-1	58:BC:27:5D:8B:A0
Test-AP-2	58:BC:27:5D:8B:B0
Test-AP-3	58:BC:27:5D:8B:C0

Importing names for all BSSIDs of the access point can be done by using this import type.

21.2.2 Running import

1. Select a separator character according to field separator character in the file to be imported.
2. If the file contains header lines that should be ignored, select correct number of lines in “Header ignored lines” drop-down menu.
3. If the file contains footer lines that should be ignored, select correct number of lines in “Footer ignored lines” drop-down menu.
4. If the file contains comment lines that start with a specific character, select a comment line start character in “Comment line start” drop-down menu.
5. Select the BSSID column number in the file. “0” means first column, “1” means second column, etc. **BSSID here means access point MAC address (which has last digit zero).**
6. Select the AP name column number in the file. “0” means first column, “1” means second column, etc.
7. Select the file to be imported by clicking “Select file..” button.
8. Select “Import file”.
9. Check status of the import in “Import status” field.



Import type and properties

Import type: Access point names (last MAC digit ze...

Separator charact...:

Header ignored lin...: 0

Footer ignored lines: 0

Comment line start: None

Column type and position in file

BSSID: 0

AP name: 0

File to be imported

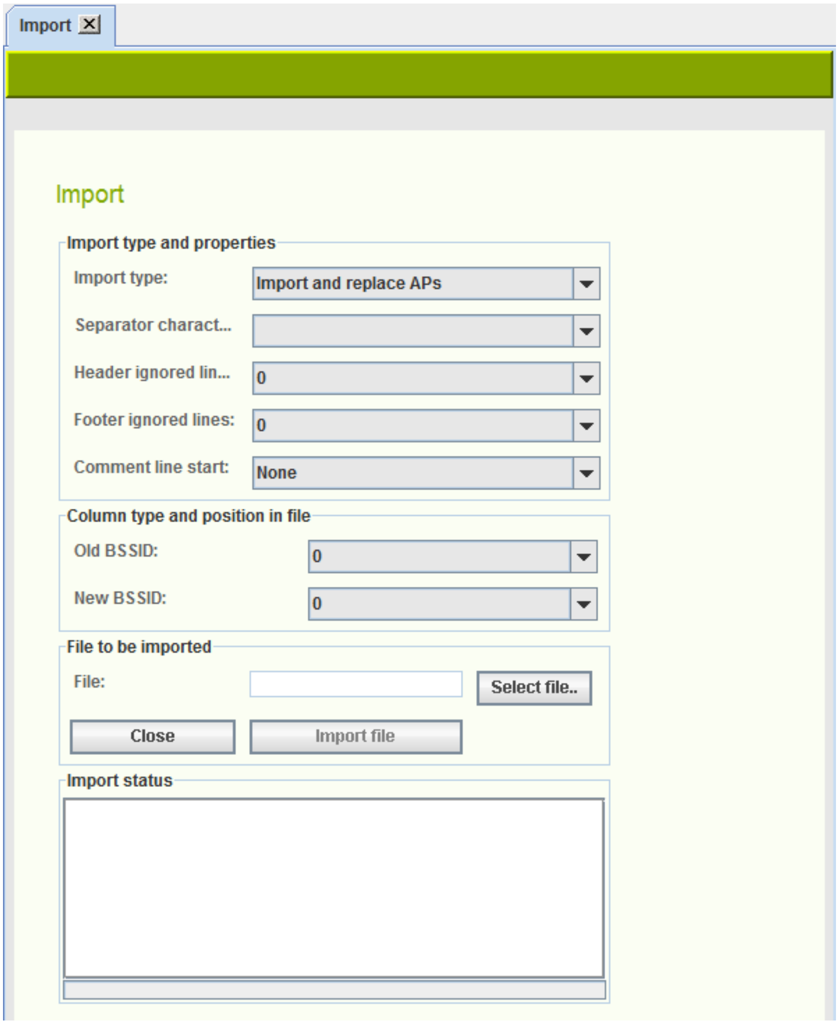
File:

Import status

Figure 72: Import access point names, last digit zero mode

21.3 Import and replace APs

This import type can be used to replace access points in the configuration. Replace is usually needed if, for example, physical access point has been replaced but the access point is wanted to be considered as the same access point in 7signal Sapphire configuration.



Import

Import type and properties

Import type: Import and replace APs

Separator charact...:

Header ignored lin...: 0

Footer ignored lines: 0

Comment line start: None

Column type and position in file

Old BSSID: 0

New BSSID: 0

File to be imported

File:

Import status

Figure 73: Replace access point by import utility

1. Select a separator character according to field separator character in the file to be imported.
2. If the file contains header lines that should be ignored, select correct number of lines in “Header ignored lines” drop-down menu.
3. If the file contains footer lines that should be ignored, select correct number of lines in “Footer ignored lines” drop-down menu.
4. If the file contains comment lines that start with a specific character, select a comment line start character in “Comment line start” drop-down menu.
5. Select the “Old BSSID” column number in the file. “0” means first column, “1” means second column, etc. This is the MAC address currently configured in 7signal Sapphire
6. Select the “New BSSID” column number in the file. “0” means first column, “1” means second column, etc. This is the new BSSID of the access point.
7. Select the file to be imported by clicking “Select file..” button.
8. Select “Import file”.
9. Check status of the import in “Import status” field.

22 EXPORTS

7signal Sapphire is capable for exporting test results and alarms to system log of the host running the Carat server. XML schemas applied can be found in `Utilities` directory of Carat distribution media.

The `Utilities` directory contains three XML schema files:

- `testresult.xsd`: Test result XML schema
- `alarm.xsd`: Alarm XML schema
- `common.xsd`: Common schema used by two former schemas

22.1 Configuring Carat system logging properties

`carat-syslog.properties` in `conf` directory of Carat installation contains Carat system logger client configuration parameters:

```
.level= INFO

# Console handler configuration
java.util.logging.ConsoleHandler.level = INFO
java.util.logging.ConsoleHandler.formatter =
java.util.logging.SimpleFormatter

# Syslog logger
com.agafua.syslog.SyslogHandler.transport = tcp
com.agafua.syslog.SyslogHandler.facility = local1
com.agafua.syslog.SyslogHandler.port = 514
com.agafua.syslog.SyslogHandler.hostname = localhost
```

Configure desired log level (default: INFO), facility (default: local1) and hostname (default: localhost).

22.2 Configuring system logger daemon

rsyslog is the default system logger daemon in RHEL/CentOS operating systems. Open /etc/rsyslog.conf file in an editor and do the following changes:

1. Uncomment following lines:

   ```
   # Provides TCP syslog reception
   #$ModLoad imtcp
   #$InputTCPServerRun 514
   ```

2. Add `$MaxMessageSize` configuration parameter:

   ```
   $MaxMessageSize 32768
   ```

   Notice that "`$MaxMessageSize`" definition **MUST** be before "`$ModLoad imtcp`" line.

3. Add rule for Carat syslog level and facility.

   If the defaults are used, add the following line to rules section:

   ```
   local1.info                    /var/log/carat-xml-output.log
   ```

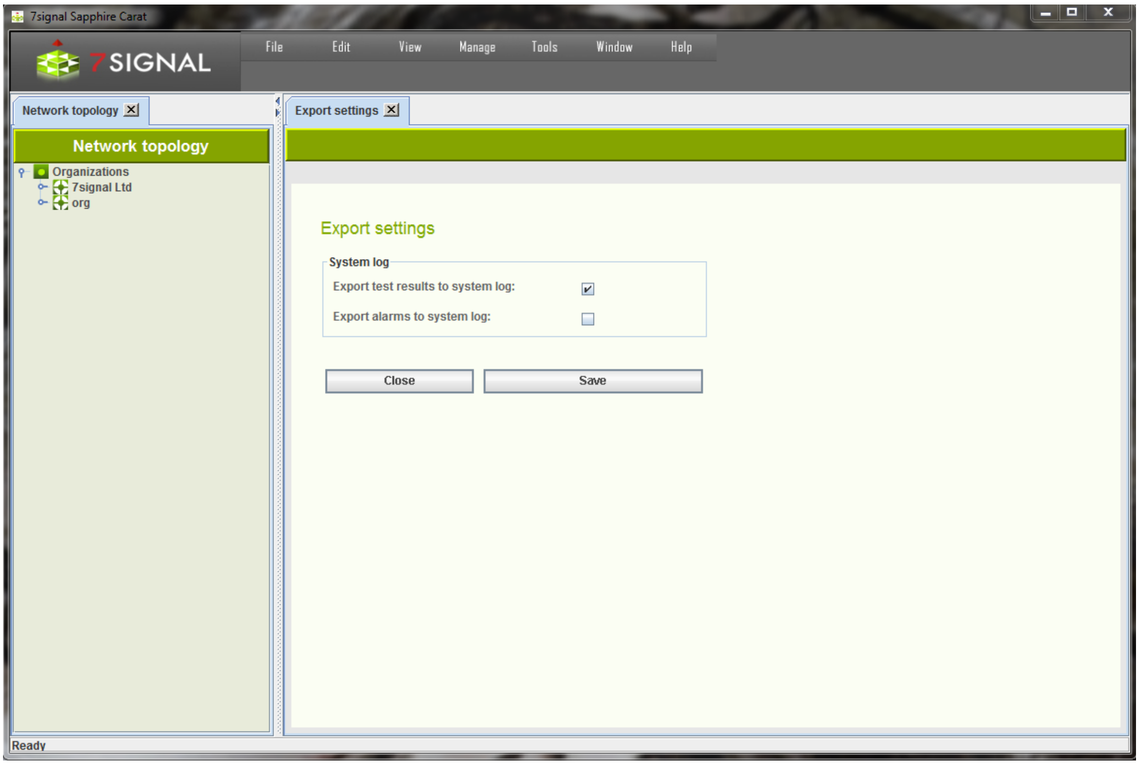
Save the file and restart daemon:

```
# service rsyslog restart
```

22.3 Exporting test results to system log

Start Management GUI and log in as solution adminstrator.

1. Select “Tool | Export…” in main menu.
2. Select “Export test results to system log” checkbox
3. Click “Save” button.



Export settings

System log

Export test results to system log: ☑

Export alarms to system log: □

Figure 74: Configuring XML alarm export

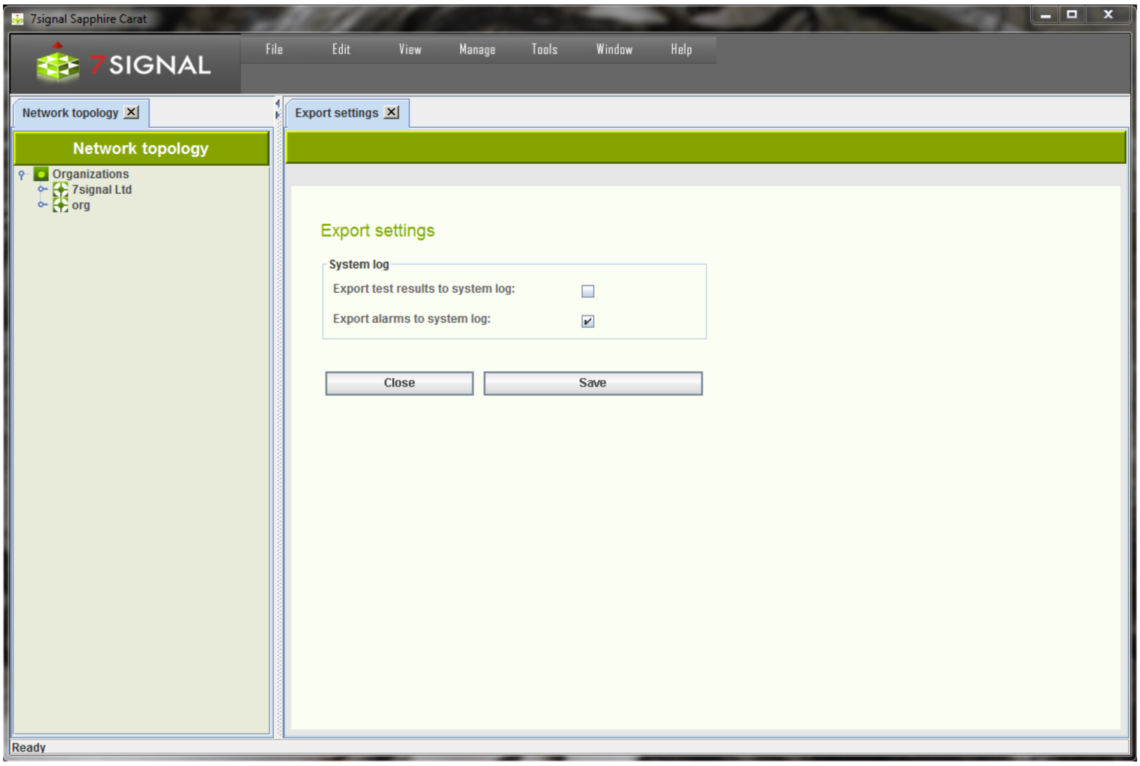
If automated tests are configured and running, test results start to appear in configured system log file:

```
Dec  4 15:31:34 localhost INFO: <?xml version="1.0" encoding="UTF-8"
standalone="yes"?><TestResultType><TimeStamp>2013-12-
04T15:31:34.057+02:00</TimeStamp><Type>active</Type><Eye><Name>eye244</Name><Id>58</Id><
/Eye><TestName>RTTPing</TestName><PingTestResult><AttachTimeMilliSeconds>0</AttachTimeMi
lliSeconds><DHCPRetrievalTimeMilliSeconds>0</DHCPRetrievalTimeMilliSeconds><LocalIPAddre
ss>10.10.10.244</LocalIPAddress><GatewayIPAddress>10.10.10.1</GatewayIPAddress><Associat
ionTime>0</AssociationTime><AuthenticationTime>0</AuthenticationTime><NetworkInterface>E
thernet</NetworkInterface><AttachSuccess>false</AttachSuccess><IPSuccess>false</IPSucces
s><AuthenticationSuccess>false</AuthenticationSuccess><AssociationSuccess>false</Associa
tionSuccess><Status>Ok</Status><PayloadBytes>32</PayloadBytes><Sonar><Name>vesku</Name><
Id>1</Id></Sonar><Antenna>0</Antenna><Channel>0</Channel><PingTestCategoryResult><Indivi
dualPingTestResultEntry><PingStatus>OK</PingStatus><ElapsedTimeMilliSeconds>1</ElapsedTi
meMilliSeconds></IndividualPingTestResultEntry></PingTestCategoryResult></PingTestResult
></TestResultType>
Dec  4 15:31:35 localhost INFO: <?xml version="1.0" encoding="UTF-8"
standalone="yes"?><TestResultType><TimeStamp>2013-12-
04T15:31:35.105+02:00</TimeStamp><Type>active</Type><Eye><Name>eye244</Name><Id>58</Id><
/Eye><TestName>RTTPing</TestName><PingTes…
```

22.4 Exporting alarms results to system log

Start Management GUI and log in as solution adminstrator.

4. Select “Tool | Export…” in main menu.
5. Select “Export alarms to system log” checkbox
6. Click “Save” button.



Export settings

System log

Export test results to system log: □

Export alarms to system log: ☑

Figure 75: Configuring XML alarm export

If automated tests are configured and running, test results start to appear in configured system log file:

```
Dec 23 14:44:50 localhost INFO: <?xml version="1.0" encoding="UTF-8"
standalone="yes"?><AlarmType><AlarmName>Noise Level
Exceeded</AlarmName><State>Acked</State><RaiseTime>2013-12-
23T14:20:28.796+02:00</RaiseTime><AckTime>2013-12-
23T14:44:50.425+02:00</AckTime><Severity>Warning</Severity><Gpt>16</Gpt><Spt>32</Spt><Ac
cessPointAlarm><AccessPoint><Name>AP_serverihuone</Name><Id>12</Id></AccessPoint><Report
ingEye><Name>eye244</Name><Id>58</
Id></ReportingEye><AccessPointAddress>58:BC:27:59:CC:20</AccessPointAddress><NetworkId>1
</NetworkId><AdditionalInfo>Channel: 48 Antennas: 1 2 3 4 5 6 7
</AdditionalInfo></AccessPointAlarm></AlarmType>
com.sevensignal.server.carat.businesslogic.northbound.syslog.SyslogService eventOccurred
…
```

23 CHANGE EVENTS

There can be events on wireless networks that impact measurement results of 7signal Sapphire. Such events can be e.g. controller software update, configuration changes in access points, power level changes etc. Because the changes affect to measurement results, 7signal Sapphire provides a method, *change event framework*, for attaching change information to measurement results.A change event can be logged for

- access points
- access points managed by specific Eye
- Eyes
- wireless networks
- wireless networks on specific service area
- links

A change event consist of a timestamp, change name and change description. A change event is visible in Sapphire Analyzer time-axis charts as a vertical line.

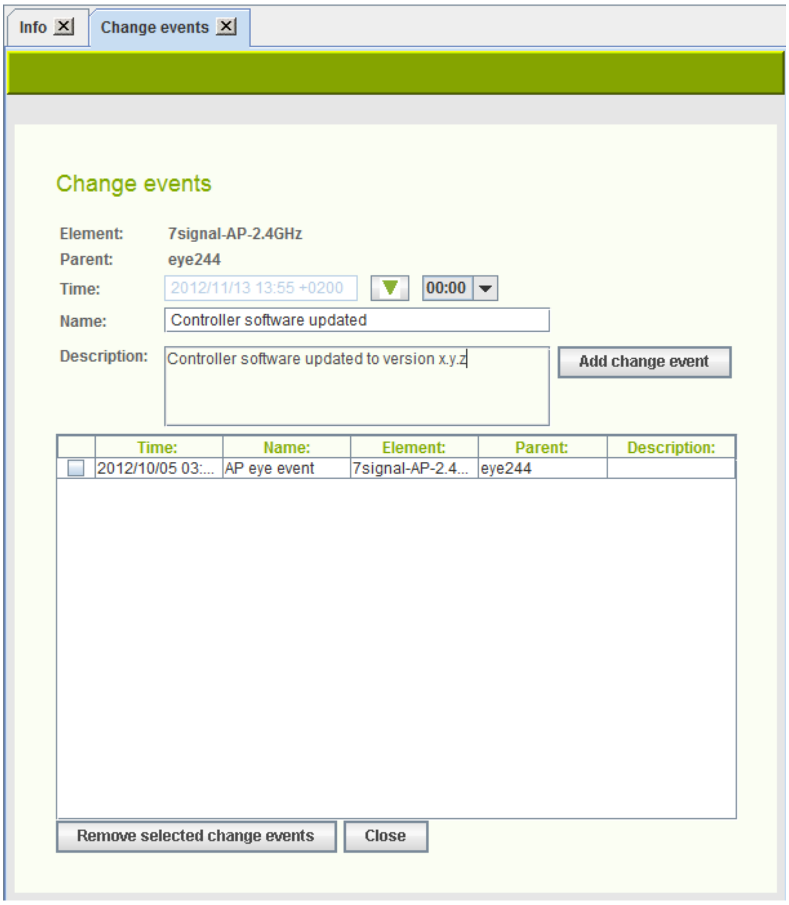
Which change events are shown in Analyzer charts depends on used area aggregation:

Table 15: Change event to area aggregation map

Change event reported for:	**Visible in Analyzer with area aggregation:**
Access point	AP DestAP ClientAP QosAP APGroup
Access point under specific Eye	APEye APEyeAnt
Eye	Eye EyeAnt ChEye ChEyeAnt ClientEye
Wireless network	NW
Access point Eye	Link
Wireless network on specific service area	NWServ NWBandServ

23.1 Reporting change events

Change events are reported by using Management GUI.



Change events

Element: 7signal-AP-2.4GHz
Parent: eye244
Time: 2012/11/13 13:55 +0200 00:00
Name: Controller software updated
Description: Controller software updated to version x.y.z

	Time:	Name:	Element:	Parent:	Description:
□	2012/10/05 03:...	AP eye event	7signal-AP-2.4...	eye244	

Figure 76: Adding a change event

Select a desired topology element and right-click to open a popup menu:

- Access point
  - Select “Change events” to report a change event for the access points.
  - Select “Change events on this Eye” to report change event for the access point under specific Eye.
- Eye
  - Select “Change events” to report a change for the Eye.
- Link
  - Select “Change events” to report a change for the link.
- Wireless network
  - Select “Change events” to report a change for the wireless network
  - Select “Change events on this Service Area” to report a change for the wireless network on the specific service area

Change event dialog is opened. Enter information for the change event:

1. Select time of the change
   a. Select date by clicking “arrow down” button.

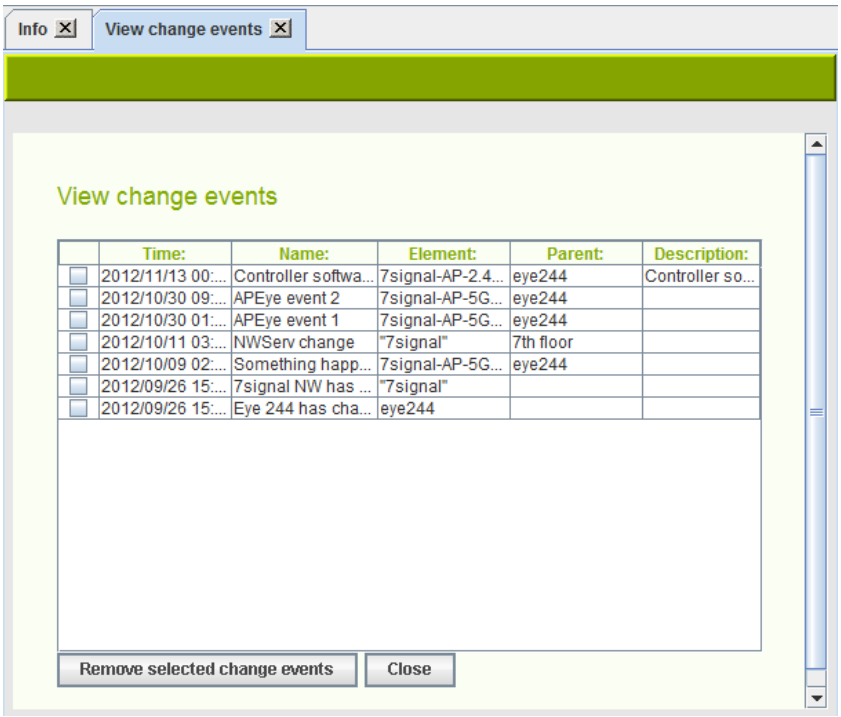
   b. Select time from the drop-down menu

2. Enter name of the change
3. Enter description of the change (optional)
4. Select “Add change event”

The added change event will appear on the list.

23.2 Viewing change events

Change events related to topology elements can be viewed by right-clicking the topology element and selecting “Change events”. Alternatively, all change events logged to the 7signal Sapphire can be viewed by selecting “View | View change events” from the main menu:

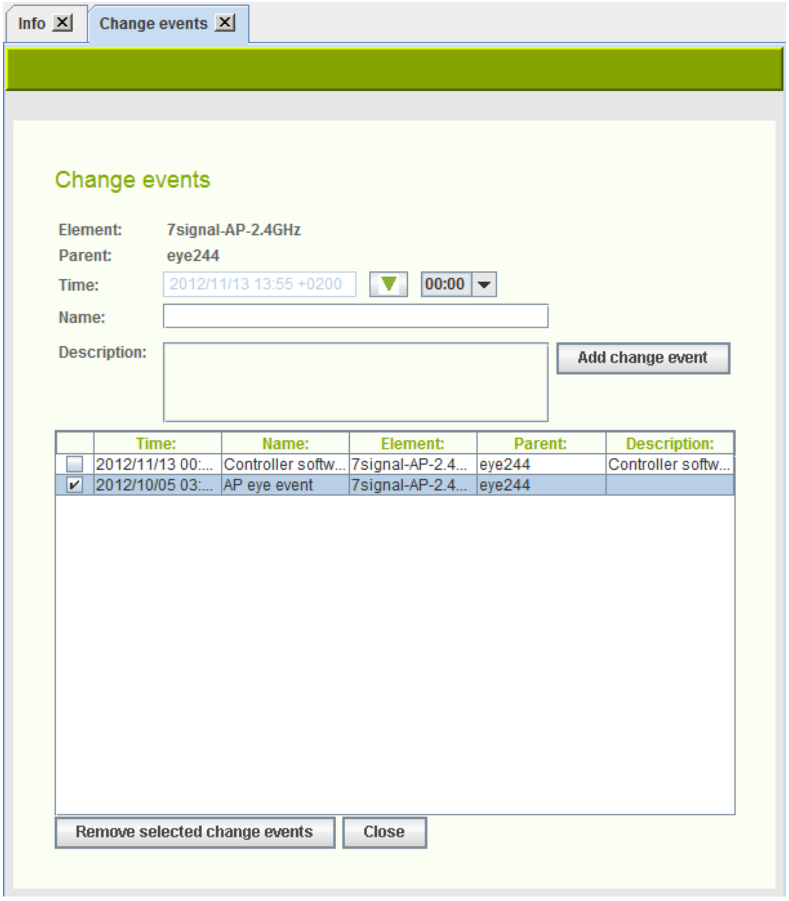


View change events

	Time:	Name:	Element:	Parent:	Description:
☐	2012/11/13 00:...	Controller softwa...	7signal-AP-2.4...	eye244	Controller so...
☐	2012/10/30 09:...	APEye event 2	7signal-AP-5G...	eye244	
☐	2012/10/30 01:...	APEye event 1	7signal-AP-5G...	eye244	
☐	2012/10/11 03:...	NWServ change	"7signal"	7th floor	
☐	2012/10/09 02:...	Something happ...	7signal-AP-5G...	eye244	
☐	2012/09/26 15:...	7signal NW has ...	"7signal"		
☐	2012/09/26 15:...	Eye 244 has cha...	eye244		

23.3 Removing change events

Change events can also be removed from 7signal Sapphire.



Change events

Element: 7signal-AP-2.4GHz
Parent: eye244
Time: 2012/11/13 13:55 +0200 00:00
Name:
Description:

	Time:	Name:	Element:	Parent:	Description:
□	2012/11/13 00:...	Controller softw...	7signal-AP-2.4...	eye244	Controller softw...
☑	2012/10/05 03:...	AP eye event	7signal-AP-2.4...	eye244	

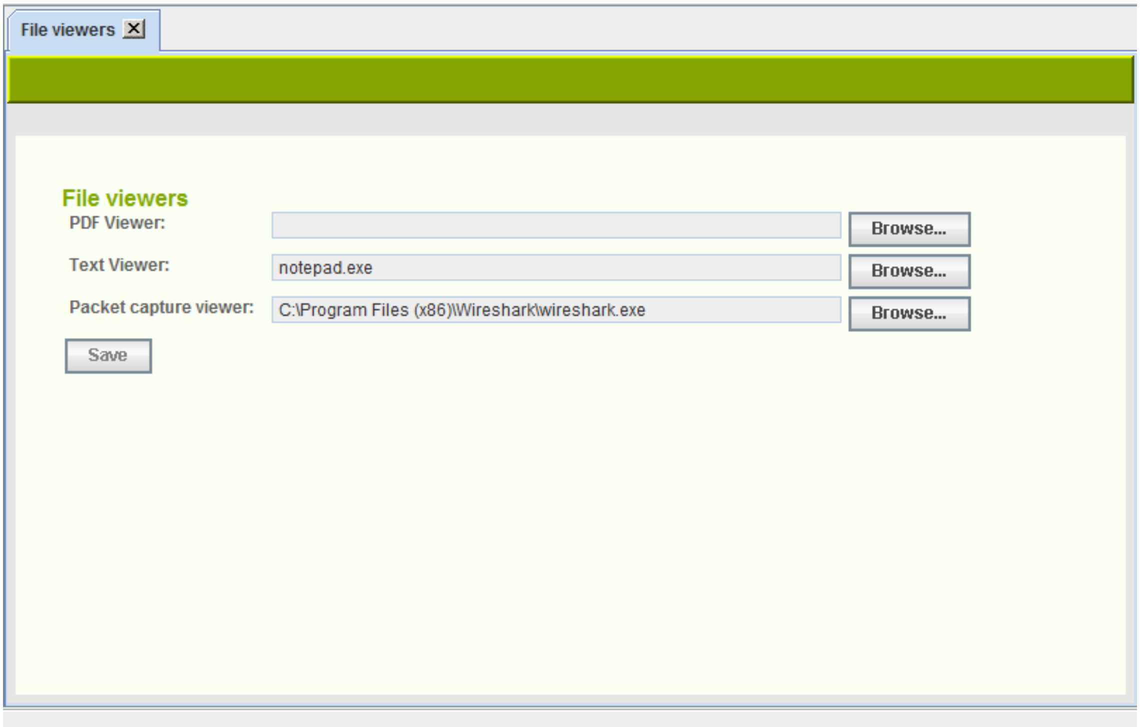
Figure 77: Removing change events

1. Open
    a. change event dialog of the desired topology element.
    Or
    b. view change event dialog from “View | View change events”
2. Select change events to be removed from the list by ticking check boxes
3. Select “Remove selected change events”

24 VIEWER SOFTWARE

Test result information and other results can be transferred outside Carat in spreadsheet format and as raw or delimited text and PDFs. You can select the applications you want to use to process these files in Carat. Packet capture viewer application is also defined in this dialog.

1. From the top menu bar, select “Edit | Configure tools”
2. The installed applications are displayed on the right
3. To change the applications, click “Browse”
4. Locate the application in the Carat server file system and select “Open”
5. Click “Save”



File viewers

PDF Viewer:

Text Viewer: notepad.exe

Packet capture viewer: C:\Program Files (x86)\Wireshark\wireshark.exe

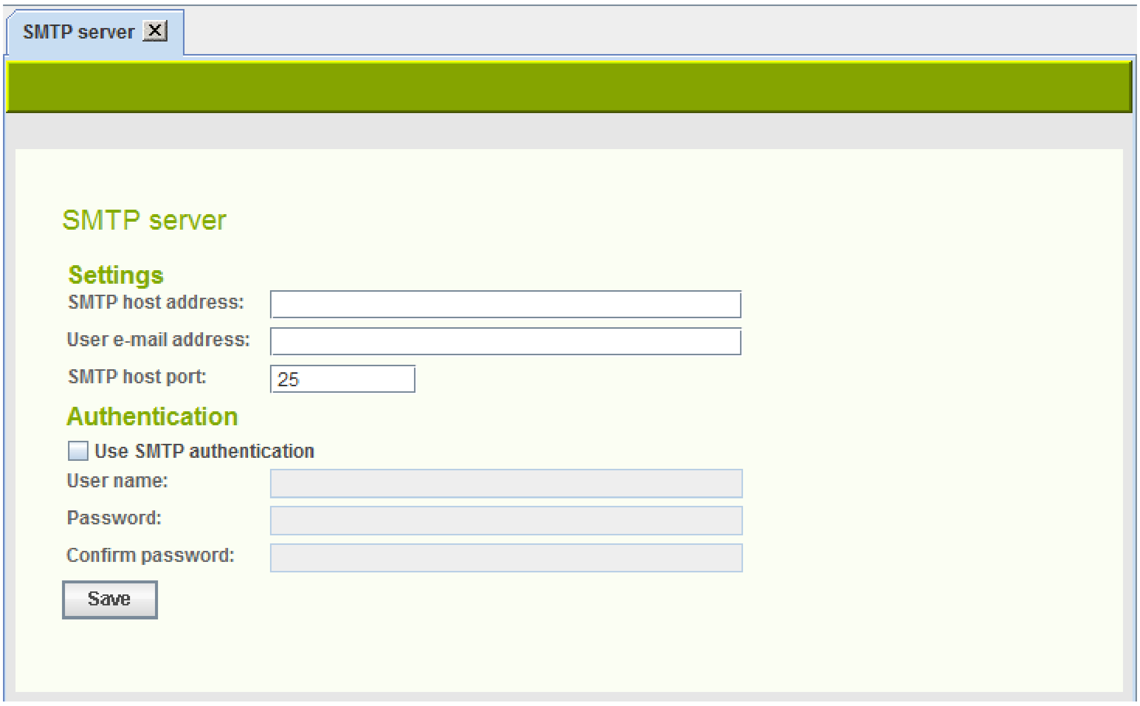
Figure 78: File viewer configuration

25 EMAIL SERVERS

In order to enable sending of automated reports and alarms to email addresses, the email server has to be configured. This setting is only for the SMTP server, the email account information is given in each of the features using the SMTP server.

> There can be only one SMTP per organization. Solution Administrator has visibility to all SMTP servers but local Administrators and Configurators may add only one SMTP server.

1. From the top menu bar, select "Edit | Mail server configuration"
2. Enter the SMTP server's address
3. Enter the e-mail address that is used as the sender of the emails
4. Enter the SMTP port to use
5. Enter a username and password, if required by the SMTP server
6. Click "Save"



SMTP server

Settings

SMTP host address:

User e-mail address:

SMTP host port: 25

Authentication

□ Use SMTP authentication

User name:

Password:

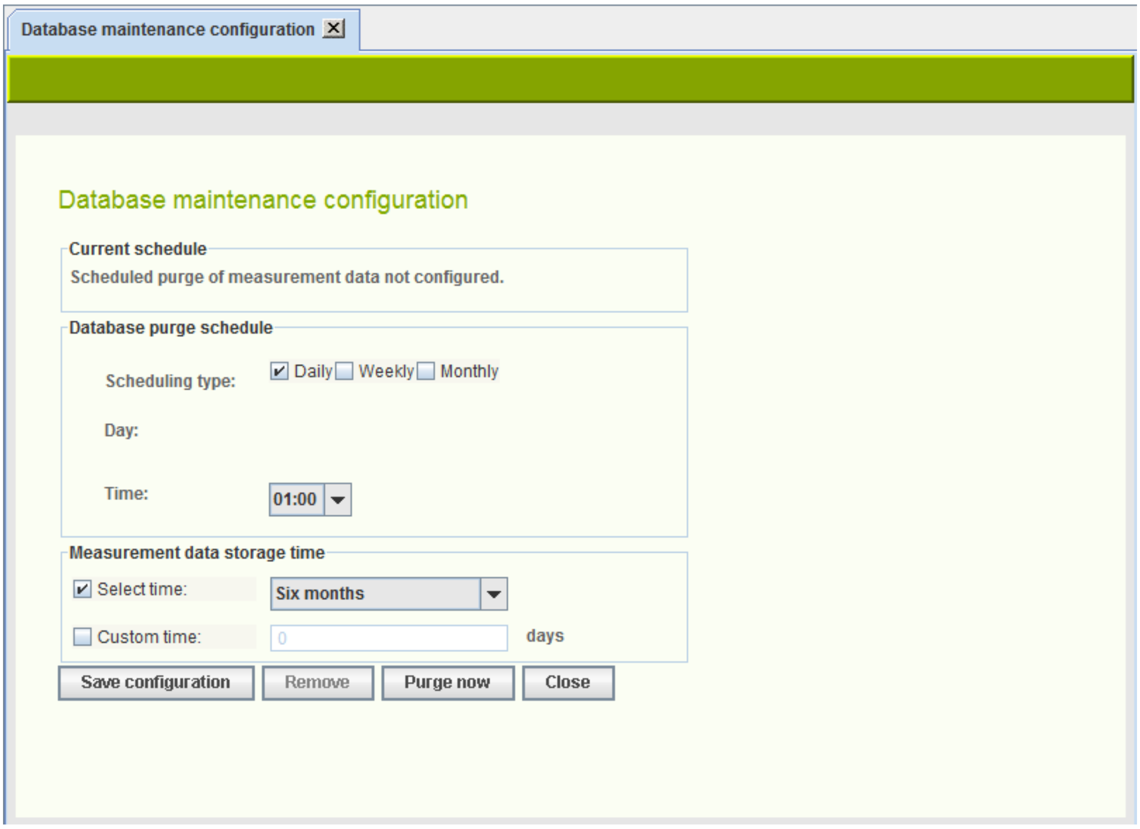
Confirm password:

Figure 79: Mail server configuration

26 DATABASE MAINTENANCE

26.1 Measurement data purge

In order to save disk space it is possible to purge old measurement data from the database. Available purge options are scheduled purge and instant purge.



Database maintenance configuration

Current schedule
Scheduled purge of measurement data not configured.

Database purge schedule
Scheduling type: ☑ Daily □ Weekly □ Monthly
Day:
Time: 01:00

Measurement data storage time
☑ Select time: Six months
□ Custom time: 0 days

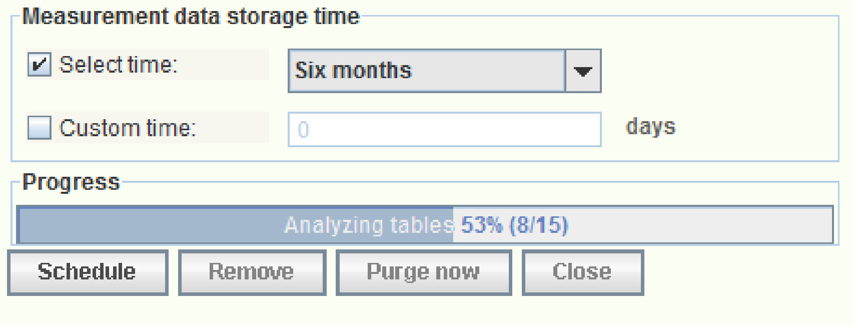
Figure 80: Database maintenance configuration

1. Select “Manage | Database maintenance” from “Manage” menu
2. In order to schedule data purge
    a. Select daily, weekly or monthly schedule
        i. If selected monthly, select day of month and time
        ii. If selected weekly, select day of week and time
        iii. if selected daily, select time
    b. Select appropriate data storage time
        i. Select time from drop-down menu
        ii. Alternatively, a custom number of days can be entered
    c. Select “Schedule”
3. In order to purge data instantly
    a. Select appropriate data storage time
        i. Select time from drop-down menu
        ii. Alternatively, a custom number of days can be entered

   b. Select “Purge now”

   c. Progress can be followed from progress bar.

4. Select “Close”



Measurement data storage time

☑ Select time: Six months

□ Custom time: 0 days

Progress

Analyzing tables 53% (8/15)

Figure 81: Instant measurement data purge ongoing

> If the database contains huge amount data that is going to be purged, the purge process may take very long time, even several days.

26.2 Database backup

It is possible to backup databases in 7signal Sapphire. Given a proper backup, the system state may be recovered completely in case of system crash. There are two remarkably different alternatives and an option not to backup the database. The default in 7signal Sapphire is no backup. While this option is known to be non-optimal for any production environment, it is chosen as default to force every organization to define own backup policy.

26.2.1 Backup options

> The backup process will use /tmp directory by default and take a lot of disk space. It is highly recommended that the default backup work directory is changed to directory residing on a large file system (not the file system on which the actual database resides). The directory can be changed with 7db-utility.
>
> Example:
>
> ```
> # 7db backup workdir set /largefilesys
> ```

Automated backup with server downtime

Backup with downtime is a circadian backup that pauses the measurements by stopping the Carat server and closing the underlying database connections. In quiescent mode a full backup of the database is made and stored to the desired location in the Carat server file system. The user is responsible for managing the backup files, moving and purging and so on. This type of logging is later referred as offline backup.

Example:

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

Automated backup without server downtime

Online backup is a circadian backup that keeps 7signal Sapphire in production while creating the backups.

> Database logging method must be archival logging.

Example:

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

Manual backup

Circular logging

Sapphire processes will be stopped during backup process and automatically restarted after backup has been created.

Example:

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

Archival logging

Sapphire processes will not be stopped during backup process.

Example:

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

26.2.2 Database logging

In short, the logs of a database system are the most precious. It is justified to say that the logs are the database as they are written first and the tables are updated after that.

IBM DB2 provides alternative logging methods that affect the backup options. So called 'circular logging' method keeps the size of the logs very predictable. The other option used in 7signal Sapphire is so called 'infinite archive logging'. This is very flexible a logging method provided that there is a special file system available. Practically the file system must not fill up ever.

The default logging method in 7signal Sapphire is 'circular logging'.

Purging database logs

Circular logging

There is no need for purging in case of circular logging. The default logging method in 7signal Sapphire is 'circular logging'.

Infinite archive logging

There is one secure way of purging the log files in the infinite archive directory. Offline backup has to be done and this comes with price of the 7signal Sapphire halt. Offline backup provides one single and unique point-in-time to be restored later. Once the offline backup exists, the log files in the infinite archive directory become obsolete and may be removed.

The other option comes with no warranty whatsoever. The option is to keep 7signal Sapphire running and to delete log files in the infinite archive directory. To understand what files are likely to be unused, the active log files has to be followed to see the time to fill up a single log file and then deduce what infinite archive files might be available for deleting . If one chooses this option, setting the safety margins reasonably high is advisable.

In case there is both a system crash and a log file has been deleted too early, the recovery shall never be able to finish. In this case, the only consistent system stage is available at offline backup time.

The automated reporting lessens the impact of possible data loss if used in detail and frequently. However, possibility to measurement drill-in analysis is lost as well as any change in the network topology and other management information.

The infinite archival logging is provided in order to support online backups (see below) but it should also be seen as a method to make system run longer automatically without user interruption. However, the system has to be maintained and administered. It is outside of the scope of this document to fit 7signal Sapphire to IT processes of all organizations but offline backups with planned system halts are highly recommended.

26.2.3 Backup method options

Default state (not recommemded)

Essentially the 7signal Sapphire system default state is not a backup system at all but it is based on the underlying database management system's robustness, fault tolerance and basic level recovery options. In case of a permanent disk failure the data is lost. By installing the databases on RAID disks lessens the risk further.

On default state the 7signal Sapphire relies on the database management system (IBM DB2) logging. The assumptions are that the management information (Eye, access point and target network) changes are not continuous but rather sporadic. The measurements are continuous but losing few of the most recent samples is a risk that can be tolerated. Typical starting point for analysis is one week of measurements and in case of sudden system down one would lose the data until the system is fixed. And in case of system down it is expected that all the efforts shall be there to bring 7signal Sapphire and other systems online again. There shall be no special snapshots where to start operations again. It is possible to resume a state before the interrupt, possibly the system is operational with no special effort at all.

Offline backups are possible but require user actions both to shutdown 7signal Sapphire and do the actual backup.

Handicaps of the default method:

- no precise and secure backup (system state) to return to by default
- backup process is completely manual
- backup process requires downtime

Method strengths:

- least planning
- least resource consuming

First degree of backup: offline backup

Most importantly this method gives fully recoverable snapshots at the desired intervals. The disk space requirement is an issue but not extremely serious as the frequency is totally user-managed and the file size growth is easy to check (with the tools provided by the operating system, not by 7signal). The downside is the downtime as the 7signal Sapphire must be halted for the time of the backup, hence it is called offline backup. Typically this would be rather minutes than tens of minutes. Naturally all the measurements are stopped for that time.

Offline backup 1st degree is available in every install and run scenario of 7signal Sapphire. One can start offline backup with a tool or have it run by the system in a circadian manner.

Method handicaps:

- backup process requires downtime

Method strengths:

- simple to recover
- recovered system state is thoroughly consistent

> TIP: offline backup is suitable for environments that require automated backup but do have neither special backup policy hardware nor other extensive resources.

2nd degree of backup: online backup

The requirement for the online backup is that infinite archive logging is enabled.

When online backup is operational, the most significant benefit is the ability to run circadian backups online i.e. 7signal Sapphire remains operational and continues testing while creating the backup. As opposed to offline backup, the system is online all the time producing measurements.

The first and the most important assumption is that there is a storage device available that in practice is a so-called endless device. 7signal cannot and shall not guarantee any checks on the device but it is assumed to be available all the time and have the capacity for massive data transfers. The user is responsible for the storage capacity.

> NOTE: backups are not done incrementally in any case. This means that over time the needed to dump the database increases but more importantly the disk space requirement increases continuously.

NOTE: use of backup systems requires planning and administration i.e. continuous effort from the administrator. This area is outside of 7signal scope, 7signal encourages clear planning on the issue.

During installation there shall be various destination folders inquired by the install script. The folders are for logs, for backup files etc. As complex as online backup may sound, the setting of the online backup is easy. To maintain and keep it available and functional requires IT support that is beyond the scope of 7signal guidance.

Behind the scenes the technology relies completely on IBM DB2 backup system and 7signal provides interface that covers and automates IBM interface to support 7signal databases.

TIP: there are environments that require separate hardware for backups. If possible, 7signal Sapphire should be integrated (on file system level) to these.

TIP: with frequent and detailed automated reports the loss of measurement data becomes less drastic as the needed information may be found in the reports.

Changing log settings

Install time gives the option to set all the backup related settings including log setup.

To change the settings while the system is installed and in production later, please use the tool **7db** and the **logsetup** sub-command. Complete guide to 7db tool is in the appendix of Deployment Guide.

Managing backup levels

By default the system is in default state, no automated backups at all. Any change to that state would require more resources and administration that should be planned separately.

In case one has changed the default settings – either by giving such install parameters or issuing the needed commands after the installation - the following operations return the initial state:

1) stop circadian backups
2) set logging to circular mode

This implies that the default state means circular logging without circadian backups.

File system settings for the database

There are three elements that require – optimally separate – disk space:

1. databases
    a. measurement database
    b. management database
    c. security database
2. database logs
3. database backups

Naturally the backups must be stored separately from the logs and the databases; otherwise the value of the backups reduces significantly. The databases and the related logs are expected to be accessible easily from the hosting server but it is encouraged to use separate physical file systems for these two.

> NOTE: log files and databases residing in the same physical disk mean duplicate disk operation efforts on the same device. It is good design to separate logs and actual databases to different physical storage devices.

Changing backup settings

Install time gives the option to set all the backup related settings.

To change the settings while the system is installed and in production later, please use the tool *7db* and the *backup* sub-command. Complete guide to 7db tool is in the appendix of Deployment Guide.

Below there are example commands to give the reader an overview:

```
# 7db backup remove
# 7db backup set weekly Wed 00:30 /mnt/backups # 7db backup set daily
03:00 /mnt/backups
# 7db backup set directory /mnt/newbackups
# 7db backup set weekly Sun 01:30
# 7db backup set type online
# 7db backup now /mnt/backups online
```

26.2.4 Restoring backups

Backups are located in the user-defined directory. Backup files contain timestamp in the name; also the operating system timestamp exists.

> NOTE: the user must be aware which backup file should be used. Therefore it is essential to understand the backup system and the related files.

Based on this information one must choose which backup to restore.

Restore command is

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

> NOTE: while issuing restore command when using online backup, it might be necessary for the system to retrieve files from the infinite archive directory when the restore command is issued. The access time is affected by the physical device. If the system cannot access the files, restore shall not happen. The most recent offline backup is the alternative point of recovery.

26.3 Management database integrity check

The Carat management database may sometimes end up to inconsistent state because of power outages, operating system crashes, etc. 7signal Sapphire provides *integritycheck* tool which is used to check and repair the management database.

1. Login to the server that hosts the Carat server as root user
2. Stop the Carat server:

   ```
   # 7carat stop
   ```

3. Execute integrity check tool:

   ```
   # 7carat integritycheck
   ```

4. If the tool finds out any problems, it asks from the user whether the problem should be corrected or not. By default, answer “yes” to all questions.

Example output of integrity check tool:

```
Connecting databases..
Database connections ready.
Starting integrity check.
* Loading SLA groups..
------------------------------------------------------------------
Checking wireless networks:
* Loading networks..
* Checking networks..
 * Checking network "7signal"
 * Checking network "7signal"
* Checking network "7Guest"
------------------------------------------------------------------
Checking access points:
* Loading access points..
* Checking access points..
------------------------------------------------------------------
Checking Eyes:
* Loading networks..
* Checking Eye eye244
* Checking Eye Eye241
------------------------------------------------------------------
Check for duplicate access points:
* Loading access points from database..
* Loading networks from database
* Checking access points..
* Comparing possible duplicates against networks
------------------------------------------------------------------
Checking links and link groups:
* Loading links..
* Loading link groups..
* Loading managed access points..
* Loading peer devices..
* Loading Eyes..
* Loading locations..
* Checking links..
* Checking link groups..
* Loading links..
Delete all 'removed' state access points from the database?
y=yes/n=no: y
…
------------------------------------------------------------------
Checking alarms:
* Loading alarms..
------------------------------------------------------------------
```

```
Checking test profiles:
* Loading test profiles..
* Loading peer devices..
 * Checking test profile jee
 * Checking test profile office
 * Checking test profile scan
 * Checking test profile passive
 * Checking test profile new tests
 * Checking test profile radio env
 * Checking test profile office+new
 * Checking test profile monitor
 * Checking test profile aptraffic
 * Checking test profile dddd
```

26.4 Reorganizing measurement database

In order to maintain optimal performance of the measurement database, the database needs be reorganized periodically. This can be done e.g. before offline backup.

Login to the server that hosts the Carat server as root user and execute the measurement database reorganization command:

```
# 7db reorg meas7
```

The reorganization tool first checks if reorganization is needed for each table. If so, it executes DB2 reorganization command.

27 NAGIOS SUPPORT

7signal Sapphire supports Nagios, a commonplace open license tool for IT infrastructure monitoring.

In this case Sapphire is the object of monitoring, not the monitor itself. Therefore we assume the general concepts and usage of Nagios to be well-known to the user. If this is not the case, one may start exploring the topic from the Nagios web pages (http://www.nagios.org). Also, a recent Nagios release package is included in the delivery media of the 7signal Solution in Sonar disk and the folder named "Non-7signal Software"

27.1 Adding Sapphire host information to Nagios server

The prerequisite is that Nagios is installed and running on the host machine. In order to monitor a remote Carat server do the following steps (as a root user):

1. Modify commands.cfg file (default location: `/etc/nagios/object/commands.cfg`)
   Add:

   ```
   define command {
       command_name check_nrpe
       command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
   }
   ```

2. Create configuration file for remote machine running the Carat server to Nagios objects directory (default location: `/etc/nagios/objects`)

   File extension is cfg, otherwise the naming is free. You may use or modify the following:

   ```
   carat-host-xyz.cfg
   7signal_wqa_carat_1.cfg etc.
   ```

   Content of the file:

   ```
    define host {
        use linux-server
        host_name <host-name-of-the-monitored-server>
        alias <alias-of-the-monitored-server>
        address <IP address of the monitored server>
    }
    define service {
        use local-service
        host_name <host-name-of-the-monitored-server>
        service_description 7signal Sapphire Carat
        check_command check_nrpe!check_carat_server
   }
   ```

3. Add host configuration file (the previous step) to `nagios.cfg` file (default location: `/etc/nagios/nagios.cfg`):

   ```
   cfg_file=/etc/nagios/objects/carat-host-xyz.cfg
   ```

4. Restart Nagios server

   ```
   service nagios restart
   ```

27.2 Adding Nagios Plug-ins To Sapphire Software

The prerequisite is that client-side tools of Nagios have been installed on the host running 7signal Sapphire software. The protocol being used is NRPE. There is no SSH support concurrently.

27.2.1 Install NRPE daemon

Use online install with yum:

```
# yum install nrpe
```

27.2.2 Install toolset 'Nagios plugins'

Use online install with *yum*:

```
# yum install nagios-plugins-nrpe
```

NOTE: the following installers shall open port tcp/5666 for Nagios traffic in the firewall settings.Install Sapphire plugin

There folders named Nagios_support on both Carat and Sonar delivery disks. They contain the following files

```
7signal-Nagios-plugin-<version-info>-for-Carat-installer.bin
7signal-Nagios-plugin-<version-info>-for-Analyzer-installer.bin
7signal-Nagios-plugin-<version-info>-for-Sonar-installer.bin
```

The files are executable and totally self-contained. By running each of the file makes the respective Sapphire Nagios plugin available. The process includes configuration file creation, updates and firewall settings.

Silent install mode (option -s) uses 7signal defaults for all parameters. If this option is not used, all parameters are inquired interactively with the default setting visible.

By default, the plugin installations end up in `/opt/7signal/nagios` folder. However, the installation makes the plugins available and after this the process and operations are completely transparent to the Carat user.

27.3 Verifying Nagios Installation

Complete and operational install is achieved if Nagios GUI shows

```
check_carat_server
check_sonar_server
check_analyzer_server
```

as options for monitoring for the hosts running 7signal Sapphire software.

27.4 Removing Nagios plugins

The installation directory contains `uninstall_nagios.sh` that removes Sapphire related plugin files. The NRPE daemon stays untouched and its configuration is cleaned only for Sapphire plugins thus NRPE and other Nagios operations remain untouched.