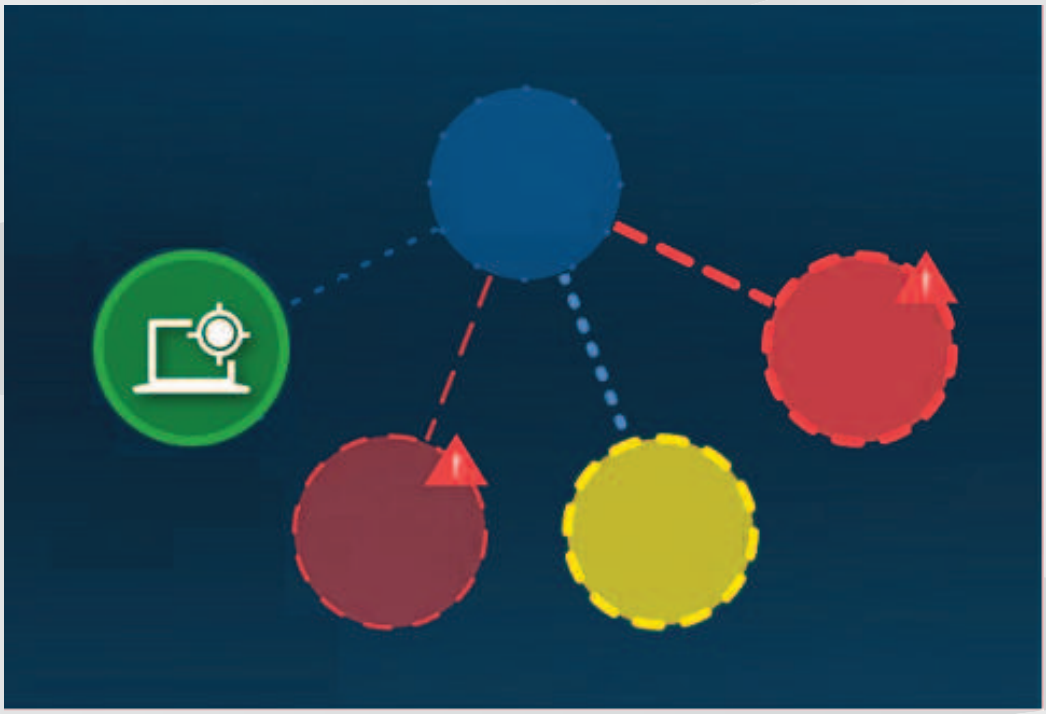
Network Docent

Diagnostics tool for OMNEO networks



en Software manual

Table of contents

1 Safety

Prior to installing or operating products, always read the Important Safety Instructions which are available as a separate multilingual document: Important Safety Instructions (Safety_ML). These instructions are supplied together with all equipment that can be connected to the mains supply.

2 About this manual

The purpose of this manual is to provide user information required for operating the Network Docent software. This manual is available as a digital document in the Adobe Portable Document Format (PDF). A related manual on this subject is:

– OMNEO Resource Guide

Refer to this manual and to other product related information at: www.boschsecurity.com.

2.1 Intended audience

This manual is intended for users of the Network Docent software.

2.2 Copyright and disclaimer

2.3 Document history

Release date	Documentation version	Reason
2017.05	V1.1	Updated version.

3 System overview

Network Docent is developed to help AV operators in their daily job. The software scans and visualizes the network environment, giving insight into all devices and cable-connections of a network-based AV system. Network Docent is able to identify and provide guidance on solving common and simple network errors that cause disruption or improper operation of the AV system. As a result, Network Docent will reduce time and effort, when installing or operating a network-based AV system.

3.1 Network Docent

Network Docent is a stand-alone utility for Windows operating systems. Key features of Network Docent are:

- Dynamic graphical overview
  - Detection and visualization of OMNEO Conference, OMNEO Intercom, OMNEO Public Address and OMNEO Pro Sound device
  - Detection and visualization of third-part AES70-devices
  - Detection and visualization of switches with LLDP and SNMP support
  - Visualization of the PC running the Network Docent software
- Error detection
  - Disconnected cables
  - Loss of power to endpoints
  - Loss of power to network appliances
  - Misconfigured network topology
  - Misallocated VLANs
  - Rogue devices on the network
- Errors and events log
  - All events and issues are reported
  - Each log entry is time stamped
- Troubleshooting
  - Guided assistance while troubleshooting issues
  - Knowledge base provides high-level information and step-by-step instructions to solve network issues
  - Compare current network situation to a previously stored scan
- Lists of connected endpoints and alerts
  - Device List
  - Device Alerts List
  - Network Alerts List

Network Docent supports OMNEO devices and devices that run LLDP (Link Layer Discovery Protocol), SNMP (Simple Network Management Protocol), AES70/OCA (a proven system control protocol for unprecedented reliability and dependability in digital audio). OCA was developed by the OCA Alliance and has been standardized by the AES (Audio Engineering Society) as AES70.

Notice!
Network installation is not part of this manual and needs to be defined in consultation with your computer administrator or local IT department.

3.2 Hardware requirements

A network-based AV system may consist of a single subnet with one or more switches, or multiple such subnets connected via one or more routers. Each node in each subnet represents a device. Each device is connected by one or more individual Ethernet cables (UTP or fiber optic) to the subnet switch or to another node in the network. For more information on this subject, see also the OMNEO Resource Guide.

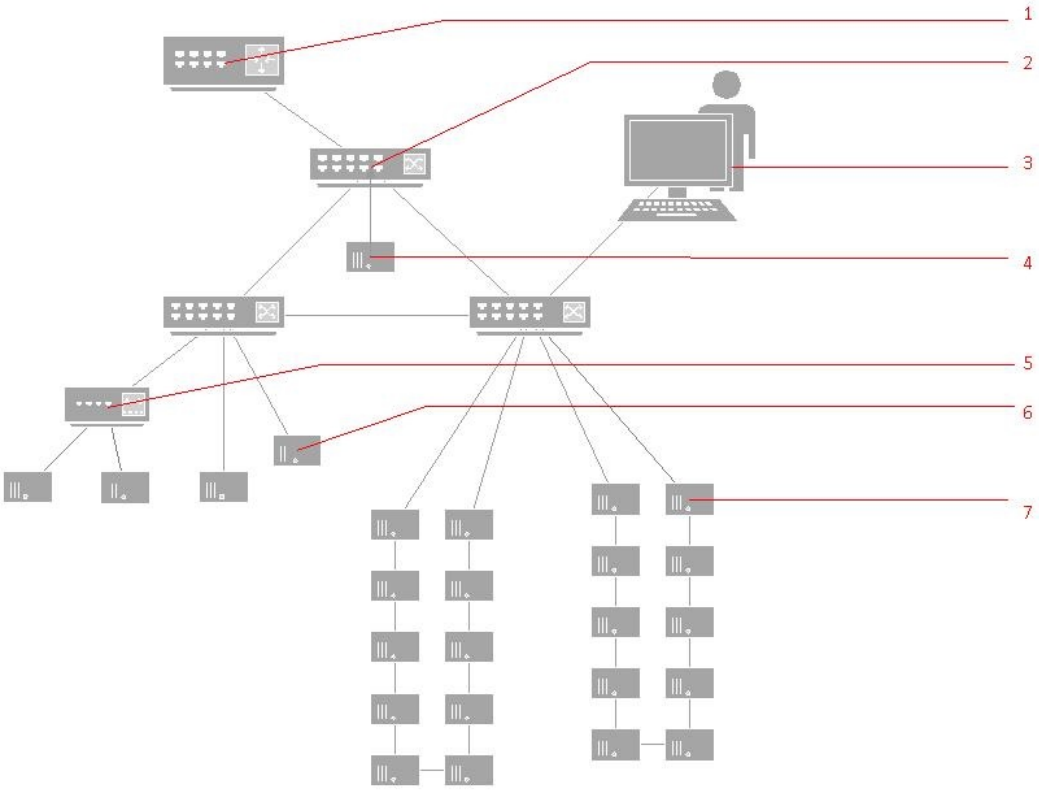


Figure 3.1: Typical audio network environment

1	Router	5	Unmanaged switch
2	Switch	6	Third party device AES70 compatible device
3	PC running Network Docent	7	OMNEO compatible device
4	ARNI-E device		

For a device to be detected by Network Docent, it must meet one or more of the following requirements:

- Bosch OMNEO device, or
- Other OCA/AES70 devices, or
- Third party device with LLDP and/or* AES70 support, or
- Third party device with SNMP support.
- Device must be connected to the same subnet as the PC, that is running Network Docent (see also *Scanning, page 24*)

  *) Devices should preferably support both LLDP + AES for best scanning results

Notice!
Installation of hardware devices is not part of this manual. Refer to the manuals that come with the devices, and to product related information on www.boschsecurity.com.

3.3 Software requirements

The minimum system requirements to run the Network Docent software on a desktop or laptop are listed in the table below. However, individual limitations might interfere with the Network Docent software, even if your computer meets these requirements. If this is the case, please consult your computer administrator.

Processor	X86 or X64 Dual core 2.4GHz
Memory	4 Gb
Free disc space	1 Gb
Operating System	Windows 7, Windows 8.1 or Windows 10; 32-bit or 64-bit
OS Updates	All Windows versions must have the latest Service Packs and updates installed.
Screen resolution	1280x720 pixels 16-bit or 32-bit color depth

3.4 Network equipment requirements

Network Docent needs to retrieve information about SNMP devices that is stored in SNMP MIB files (Simple Network Management Protocol Management Information Base). To do this successfully, Read-Only (or higher) access rights are required to these MIB files:

MIB file	**OID (Object Identifier**
RFC1213-MIB2	.1.3.6.1.2.1
LLDP-MIB	.1.0.8802.1.1.2

Network Docent supports a wide range of network topologies: star, tree, ring, mesh, and hybrid (see also OMNEO Resource Guide). Devices in a network-based AV system are physically connected to a subnet switch or to another node in the network by one or two individual Ethernet cables (UTP or fiber optic).

3.5 License requirements

While installing the Network Docent software, the **End-User License Agreement** window will show up. This window contains the BOSCH SECURITY SYSTEMS B.V. LICENSE AGREEMENT FOR SOFTWARE and other license agreements:

- BOSCH SECURITY SYSTEMS B.V. LICENSE AGREEMENT FOR SOFTWARE
- Apache License 2.0
- MIT License
- BSD 3-Clause
- ISC License

Review and optionally print a copy of the agreement, then click the **I accept the terms in the License Agreement** check box.

When using the Network Docent software, these license agreements can be found in the 'about' dialog. **Click Menu > About** to open this dialog. All license agreements are also provided in .rtf files that can be found in the Program Files folder on your Windows computer: `%programfiles%\Bosch\OMNEO\Network Docent\`

Figure 3.2: Use the slider on the right of the 'about' dialog to scroll through all licenses

4 Software installation

The Network Docent software can be downloaded from:
https://licensing.boschsecurity.com/omneo/

4.1 Downloading Network Docent

Download the file as follows:

1. The download is a zip file archive. Zip file archives have a .zip file name extension.
2. Please make sure to download the right version for your system 32 or 64 bits (pressing the hotkey Windows + Pause will open a window with information on the Windows operating system of your system).
3. Save the zip file to a folder on your Windows computer.
4. Windows will unpack the downloaded zip file archive when you right click on the file name and select **Extract**.

4.2 Installing Network Docent on a Windows PC

The extracted file is an executable (.exe) file. Double-click on the filename to start the **Installation** process.
The process guides you through the following steps:

1. Start with the Opening screen; click **Install**.
2. Windows User Account Management will ask your confirmation: click **Yes**.
3. Welcome screen, click **Next**.
4. End-User License Agreement. Review and optionally print a copy of the agreement, then click the **I accept the terms...** check box. Click **Next**.
5. Click **Install**. The install process continues. A progress bar shows the status of the process.
6. As soon as this is done, click the **Finish** button.
7. Repeat steps 5 and 6 for optional auxiliary software to be installed.
8. Click the **Close** button.

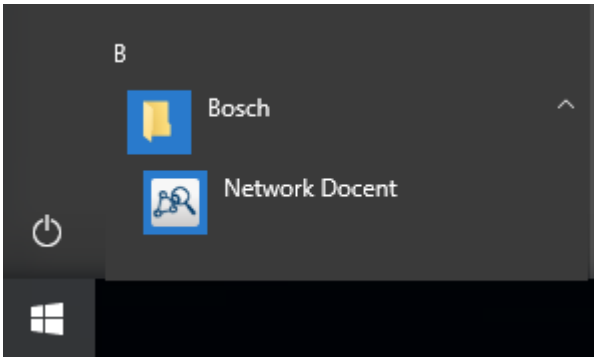


Figure 4.1: Bosch group in the Windows 10 Start menu

On the Windows Start menu you will find the group: **Bosch**. This group contains the following item(s):

– Network Docent software
– Other Bosch software (if applicable)

In general, the Network Docent software will be installed in:

`%programfiles%\Bosch\OMNEO\Network Docent`

4.3 Updating Network Docent

Check our website for new updates:
https://licensing.boschsecurity.com/omneo/
Follow the procedure as described under chapters *Downloading Network Docent, page 11* and *Installing Network Docent on a Windows PC, page 11* to download and install a new update.
If you want to install a new version of Network Docent, you do not need to uninstall the current version first. After updating a reboot of the Windows PC will be necessary.

Notice!
Network Docent's knowledge base is an integral part of the application, so updating Network Docent implies updating the knowledge base as well.

4.4 Uninstalling Network Docent

If for some reason you want to uninstall Network Docent, follow the Windows Uninstall procedure: navigate to **Control Panel** > **Software** > **Programs and Features** > select the OMNEO ControlNetwork Docent software > click **Uninstall**.

5 Getting started tutorial

This tutorial will help you become familiar with the basics of Network Docent. You will learn how to start the application, how to scan the network, and how to recognize issues.

1. Ensure that the network and all devices comply with the system requirements, as described in *System overview, page 7*.
2. Start the Network Docent software. From the Windows Start menu select: **Programs > Bosch > Network Docent**. Windows 7 users select: **All Programs > Bosch > OMNEO > Network Docent**.
3. Network Docent welcomes you with the Guided Tour dialog. The tour will guide you through the main elements of the application, and teach you how to diagnose and monitor your network. You can skip the tour by clicking the **Stop** button in the Guided Tour dialog. It is advisable to take the Guided Tour at least once, to get familiar with the application.

Notice!
If you do not want Network Docent to run the Guided Tour each time you start the application, just click the check button in the lower left corner of the dialog to disable the Guided Tour. To enable it again, see also *Application Settings, page 41*.

4. Network Docent always starts in 'offline' mode. The corresponding status is indicated in the status bar on top of the screen: 'Docent Offline'.

The status bar contains two buttons only: **Menu** on the left and **Scanning**. The Scanning button now carries the label 'Scanning Offline'.

Click the **Scanning** button. The button label changes into 'Scanning Active'. The application is now online and is scanning for supported devices in the connected network(s). The 'Docent Offline' indicator will change too, for instance into 'All Networks Online'.

While scanning, the network visualization is being populated with node-symbols, representing found network(s) and their devices. The total numbers of found networks, devices and connections are displayed on the right side of the status bar and may look like this:

After completing the scan, scanning will stay active, continuously updating the visualization.

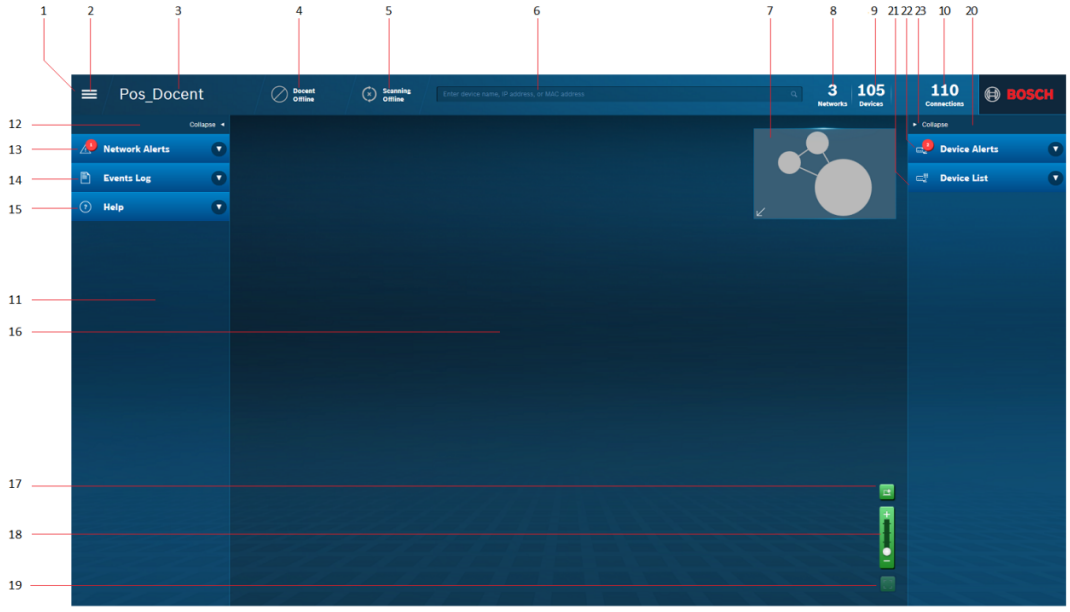


Figure 5.1: The Network Docent screen consists of a status bar, and left, center and right panes

1	**STATUS BAR**	16	**CENTER PANE (Network Visualization)**
2	Menu	17	Zoom to PC-running-Docent
3	Network snapshot name	18	Zoom slider
4	Online/offline status	19	Zoom button
5	Scanning button		
6	Search Device text box	20	**RIGHT PANE**
7	Thumbnail image of total network	21	Device list
8	Number of networks	22	Device Alerts list
9	Number of devices	23	Collapse button
10	Number of connections		
11	**LEFT PANE**		
12	Collapse button		
13	Network Alerts list		
14	Events log list		
15	Help topics		

5. The Network Visualization supports four levels of zooming and grouping (read chapter 6 for more details on this subject). The highest zoom-level or 'device-level' shows all devices, each represented by a node-symbol. Zooming out causes devices to be grouped together in large group node-symbols, thus giving a simplified overview of the full network with less detail. The lowest or 'basic zoom-level' usually shows just a few node-symbols, representing the PC running Network Docent and the networks (see also *Zooming, page 23*).

Use the zoom slider in the lower right corner of the visualization to control the amount of detail and grouping. Or use the mouse wheel, or the plus and minus keys of your keyboard instead.

Figure 5.2: Zoom slider set to 'device level'

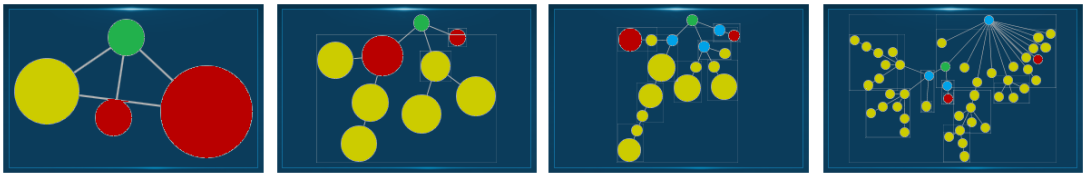


Figure 5.3: Zooming in via four zoom-levels ungroups more parts of the network'

Toggling the **Zoom button** beneath the zoom slider offers a fast route to basic zoom-level and device-level.

6. If zooming in enlarges the visualization to a size that does not fit the screen, you can check out the upper right corner of the Network Visualization, showing a thumbnail image of the total network. Inside this image a gray rectangle represents the visualization area.

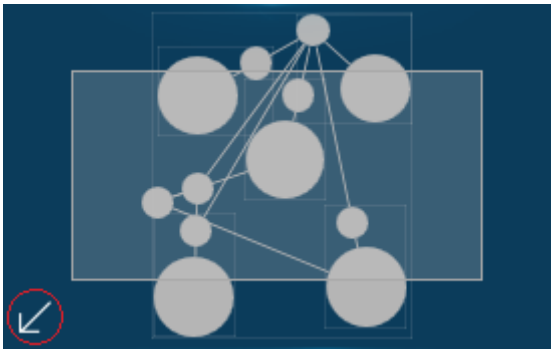


Figure 5.4: Thumbnail image - Gray rectangle represents the visualization area, click the arrow to enlarge

The thumbnail image is part of the four ways to make invisible parts visible:

- Zoom out, by using the zoom slider, or the mouse wheel, or the plus and minus keys of your keyboard.
- Click in the Network Visualization and keep the mouse button pressed, while shifting your mouse to other parts of the visualization.
- Click and drag the gray rectangle in the thumbnail image to other parts of the network. Click the arrow in the lower left corner of the thumbnail image, to enlarge the image.
- Press the Ctrl-key while zooming in or out. This will make all node-symbols smaller or bigger.

7. Each device in the visualization is a network node, represented by node-symbols. The PC that you are working on, and that is running Network Docent,Network Docent is one of the network nodes, and is represented by this node-symbol (green or yellow):

Clicking the **Zoom to PC button** (see below) above the zoom slider will make the Network Visualization zoom in to this node-symbol.

Every other device or group of devices is shown by a colored node-symbol, each node-symbol mentions the status of the corresponding device:

Connected

Disconnected

New Device

Duplicate IP address
Subnet mask mismatch
Gateway mismatch

Unknown device
Unmanaged switch
Unknown Network Path

Colors and outlines of the node-symbols emphasize the status of the corresponding device, group or network(s):

green	no issues (solid outline)
blue	unmanaged switch (solid outline) unknown network path (dotted outline)
yellow	warning alert (dashed outline)
red	error alert (dashed outline plus warning sign)

Connections between nodes are represented by one of the following line types:

green solid	connection to device or group with no issues
blue dotted line	connection to an unknown network path
red dashed line	connection to device or group with critical issue(s)
two parallel lines	glitch free connection

Clicking a node-symbol in the visualization will highlight it. Unless the highlighted node-symbol carries an 'Unknown' status, detailed information on the corresponding device is displayed in the Device List in the right pane.

Notice!
The dotted or dashed property of connections and node-symbols has no additional meaning, other than helping users with color-blindness distinguish the differences.

Notice!
After scanning a network for the first time, most devices will be represented by yellow node-symbols, carrying the status **New device**. Examine the new devices on the network. Unwanted devices might influence the network performance, security and functionality, and must be removed. Other new devices must be **Approved**. Later in this manual you will learn on how to do this (see also *Network Docent - Expert reference, page 23* and *Troubleshooting, page 43*).

Notice!
OMNEO and SNMP devices have a security mechanism that prevents them from being scanned by unauthorized systems. Network Docent will detect them and display them as 'Unconnected'. To enable Network Docent gathering more information about these devices, their credentials have to be set. See also *Network snapshot settings, page 37*.

8. All discovered devices on the network(s) are also listed in the Device List on the left. Click the Device List button to expand the list:

Each device carries the same color coding as the device status in the network visualization. The device list shows the device names in alphabetical order, and will be segmented in locations but only if locations have been assigned first. To add locations, see also *Add locations, page 28*.
As shown in figure 5.5 clicking a device in the Device List provides detailed information on that specific device, like MAC address, IP address, connections etc. Click the green **Zoom to Device** button to highlight and locate the device in the network visualization.
The detailed device information also becomes visible when clicking a node-symbol in the network visualization. However, devices with an 'Unknown network path' status lack this kind of information.

Figure 5.5: Example of the Device List (left) and detailed information on the clicked-on device (right)

9. The **Device Alerts** list is like the Device list, containing only devices with a red or yellow alert. Click the **Device Alerts** button to expand the list; the number in the red circle represents the total number of devices with an alert:

Clicking a device in the Device Alerts list provides detailed information on that specific device in the right pane.

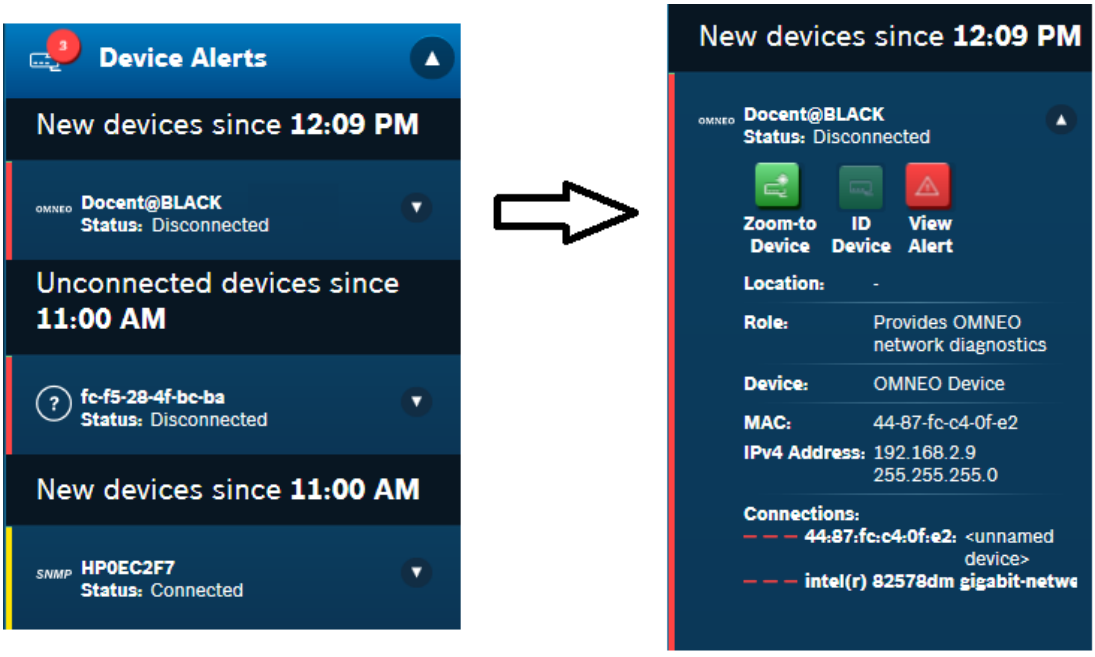


Figure 5.6: Example of the Device Alerts list (left) and detailed information on the clicked-on device (right)

10. If the network has any issues, these are listed on the left side of the screen in the **Network Alerts** list. The Network Alert button will show the number of active alerts in a red circle. Click the **Network Alerts** button to see all active alert(s):

The list shows the gravity of each issue plus the moment when it occurred for the first time. For instance, newly found devices in a network will generate an alert indicating new devices have been detected. The severity of this alert is indicated by a vertical yellow ribbon, meaning 'Warning'. Red ribbons indicate critical issues.

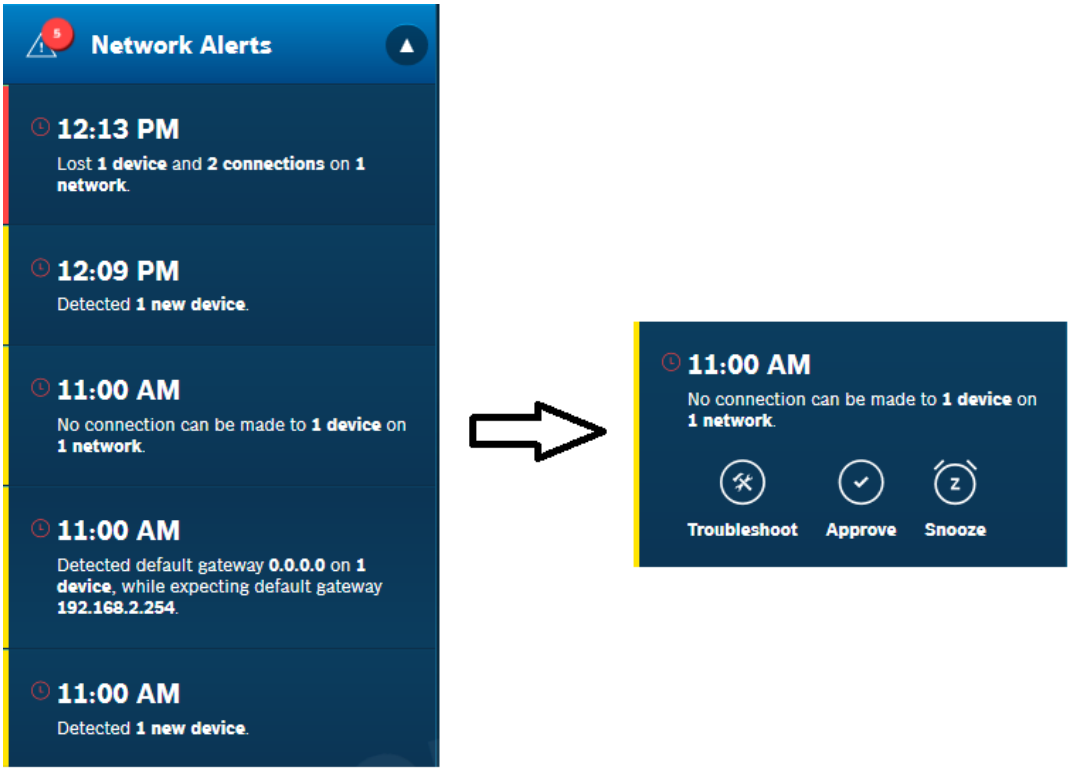


Figure 5.7: Clicking an alert in the Network Alerts list (left) reveals three buttons (right

Clicking an alert highlights all applicable node-symbols in the network visualization, and also reveals three buttons, allowing you to take action on that specific alert:

- **Troubleshoot:** the alert is explained in a help text that will help you solve the issue.
- **Approve:** the alert is accepted as being an okay network situation.
- **Snooze:** postpone action to a later date.

11. Click **Troubleshoot** to read about possible causes and solutions in the **Help** pane.
12. Clicking the **Expand the View** button will copy the Help contents to a tab in the center pane of the screen.

Close this pane by clicking the cross in the Help tab on top of the pane.

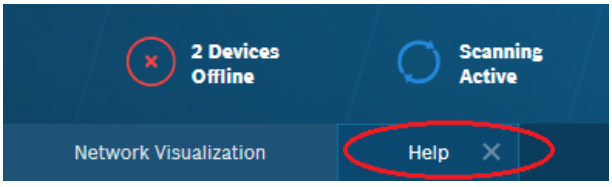


Figure 5.8: Expanding Help creates a new tab in the middle pane of the screen

Additional troubleshooting information can be obtained by clicking one of the two green buttons on the bottom of the Help pane: **Search for more solutions** and **Export details for tech support**. See also *Technical support exchange, import, export, page 39*.

Figure 5.9: The route to solutions: clicking the Troubleshoot button in a Network Alert opens the Help pane

13. Network Docent Network Docent keeps track of events and errors that occur on the network. Click the **Events Log** icon on the left side of the screen.

A list of the most recent events opens. Each event is marked with a description and its severity: Critical, Error or just a Warning. See also *Events log, page 33*.

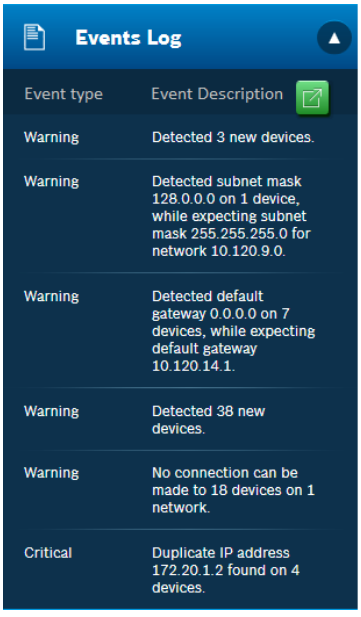
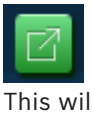


Figure 5.10: Events and errors are logged

For better readability, click the **Expand the View** button or click one of the events in the Events Log list.



This will open the Events Log contents in a new tab in the center pane of the screen. Close this pane by clicking the cross in the **Events Log** tab on top of the pane.

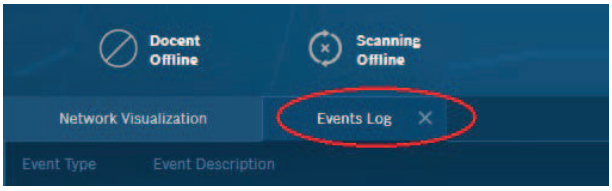


Figure 5.11: Expanding the Events Log creates a new tab in the center pane of the screen

14. To close Network Docent click the **Menu** button in the upper left corner of the Docent-window and click **Exit** (or press hotkey Alt+F4 instead).

- Click **Save** if you want Network Docent to save a 'snapshot' of the current network status for later reference and troubleshooting.
- Click **Don’t save** if you want to exit the application without saving such a snapshot.
- Click **Cancel** if you do not want to exit and want to continue using the application.

6 Network Docent - Expert reference

Before you begin this chapter, it is assumed that you have already gone through the previous chapter.

6.1 Network visualization

Network Docent can be used to identify some of the most common issues when configuring a network for AV use. The application provides an easy to understand network visualization that represents the network's physical layout. Users can use this visualization to highlight potential issues.

6.1.1 Zooming

Network Docent 's visualization offers three ways of zooming in and out: by shifting the zoom slider, turning the mouse wheel, or pressing the plus and minus keys of your keyboard. Zooming out means grouping network elements together into a smaller number of node-symbols. Zooming in means ungrouping these network elements, and showing more detail. Zooming distinguishes four levels of detail in the displayed network visualization:

+ Basic zoom-level shows a global overview of the total network. The PC running Network Docent is shown as a node-symbol. All other devices and the network itself ideally are grouped in one large node-symbol. However, most networks consist of two or more logical network-segments, thus two or more large node-symbols are shown, each representing an IP-address range. For instance, one node-symbol stands for logical network-segment with IP-address range 192.168.0.1 - 192.168.0.16, another for 172.20.1.0 - 172.20.1.32.

++ Second zoom-level ungroups the logic network-segments on switch level. The large node-symbols now represent a switch each, including the devices connected to that specific switch.

+++ Third zoom-level ungroups managed switches and unmanaged switches, which are made visible as individual nodes; most other devices are grouped in large node-symbols.

++++ Highest zoom-level or device level: all Bosch OMNEO devices, OCA devices, computers and other detected devices are ungrouped and shown as individual nodes; all connections are shown as solid, dotted, and/or dashed lines.

Zooming in visually ungroups node-symbols. Each group is visualized by a small rectangle in the thumbnail image, enclosing the devices belonging to that specific group. See figure 6.1.

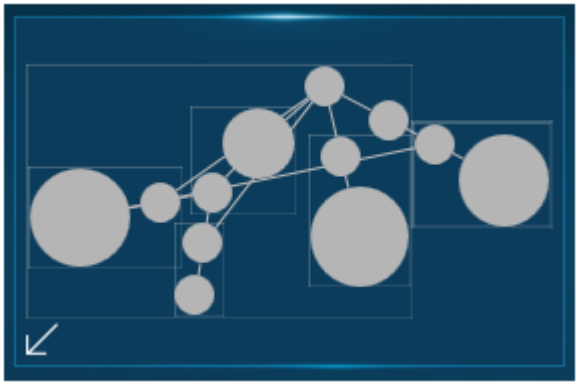


Figure 6.1: Small rectangles in the thumbnail image visualize a group

Notice!
Routers in the network visualization are displayed as switches. Devices connected to a router are not detected. See also the workarounds in *Limitations, page 26*.

Notice!
If the number of nodes is too big to fit on your screen, press the Ctrl-key while zooming in or out, using the – and + keys or the mouse wheel. This will make the node-symbols smaller or bigger.

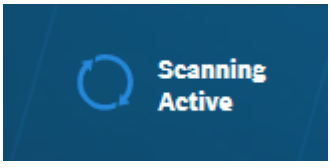
6.1.2 Network snapshot name

The name that Network Docent displays in the left corner of the status bar is the **Network snapshot** name. This name is used to save the current network configuration, and to re-open it again on a later date. When starting Network Docent for the first time, the left corner of the status bar reads: <Untitled>. See also *Save and open network snapshot, page 36* on saving, and changing this name.

Notice!
If the network snapshot name is too long and shows dots instead of characters, hover the mouse over the name to read the full name in a tool tip.

6.1.3 Scanning

Click the **Scanning** button in the status bar to start or pause the scanning process.



The button label changes into **Scanning Active**, while Network Docent is scanning for supported products in the connected network(s). All detected devices are shown with their names and status. Bosch OMNEO devices are always detected and shown.
As far as third-party devices, LLDP and SNMP support are critical factors in the scanning process. Detected devices include:

- Network switches and bridges
  - LLDP and SNMP enabled switches and bridges are detected, full information included.
  - Switches with both LLDP and SNMP disabled are considered unmanaged switches. See also *What are 'Managed switches' and 'Unmanaged switches' in the network visualization ?, page 50* about managed and unmanaged switches.
  - IP Routers are not detected by this first release of Network Docent.
- Network cabling
  - STP/UTP and fiber optic cables are detected. The cable type itself is not identified in the network visualization.
- Network topology configurations (VLANs, etc.)

  - The scanning process detects star, tree, ring, mesh, and hybrid topologies (see also OMNEO Reference Guide).
  - Wi-Fi is not supported. However, Wi-Fi devices may be detected and generally are shown as connected via an 'unknown network path'. This is because wireless devices in a wireless network are by nature connected in star topology. This kind of topology significantly decreases the amount of information that Network Docent can gather.
- Network endpoints
  - Bosch OMNEO products running both LLDP and OCA are detected, full information included.
  - Third party network devices running both LLDP and SNMP are detected, full information included.
  - Third party network devices running only LLDP are detected, MAC address included.
  - Third party network devices without LLDP are not detected, unless they are connected to devices that run LLDP and SNMP or OCA. In that case they will be shown as 'Unknown device'.

A device is shown as 'Disconnected' when:

- the device is present in a previously stored network snapshot, but is not detected in the current network situation; after approving this alert, the alert and the device disappear from the visualization.
- the device is known to be present, but Network Docent is not able to connect to it; after approving this alert, the device will remain visible in the visualization as 'Disconnected'.

The total numbers of found networks (logical network-segments), devices and connections are displayed on the right side of the status bar. After finishing, scanning will stay active, updating the visualization continuously.

Notice!
Make sure to set the security credentials for OMNEO and SNMP devices before scanning. OMNEO and SNMP devices that are detected without setting the right credentials first, will be displayed as 'Unconnected' device. See also *Network snapshot settings, page 37*.

6.1.4 Offline and Online state

The **Scanning button** in the status bar enables you to start or stop the scanning process, and - at the same time - set Network Docent online or offline. While Network Docent is offline, a corresponding status indicator in the status bar on top of the screen reads: 'Docent Offline'.

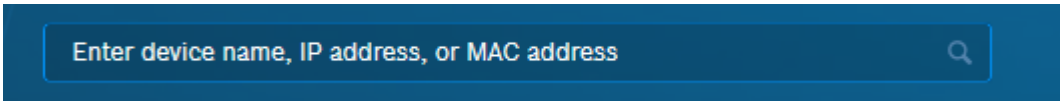
While Network Docent is online this indicator will change regularly, giving you a quick update on the network status:

Notice!
When online, Network Docent actively connects with devices in the network. This may have its impact on certain AES70 controllers in the network, due to device limitations on TCP connections.

6.1.5 Search

The **Search Device text box** in the status bar on top of the screen offers a quick way of zooming in and locating a specific device in the network:

1. Type the device's name, IP address or MAC address in the **Search Device text box**.
2. If you only type a part of the name or the address, the search function will display a list of search hits. Click the hit you want to view.
3. Network Docent will zoom to the level, on which the device is ungrouped and shown as a node-symbol in the network visualization. Quite often that level appears to be the highest zoom-level, and sometimes the third zoom-level.



Notice!
Do not use the **Search** function to track down devices with a duplicate IP address. Instead, click the corresponding alert in the Network Alerts list to highlight both devices in the network visualization.

6.1.6 Limitations

Although Network Docent supports large and very large networks, a few limitations apply:

- Maximum Number of devices = 500.
  This number includes switches, Bosch OMNEO devices, OCA devices and other audio devices. Routers are out of scope.
- Maximum number of end points = 450.
  This leaves room for 500-450 = 50 network equipment devices.
- Maximum number of network infrastructure equipment devices = 50.
  These devices link all endpoints together.
- Maximum number of subnets = 1.
  Since routers are out of scope Network Docent is limited to a single subnet environment. To get insight into other subnets you can use one of these workarounds:
  - Connect your PC to another subnet and run Network Docent.
  - Select an existing PC in each subnet and install and run Network Docent on the PC.
- Wireless devices have limitations, see also *Scanning, page 24*.

The maximum numbers have been tested and are trusted. If one or more of these numbers are exceeded, Network Docent may still appear to be working normally, but its functionality and reliability cannot be guaranteed.

6.2 Device List

The Device List shows a list of names and states of all detected devices in the network. Clicking a device name will reveal additional information about the device. Apart from the location, this information is retrieved from the devices themselves and from adjacent devices via AES70, SNMP and LLDP. The information includes:

Name

Status

Location

Role

Device

MAC address

IP address

Connections

This information is read-only and cannot be changed by Network Docent (except Location). If changes are to be made, refer to the manual of the device on how to do this.
If the device has an issue, the device information is marked with a red or yellow vertical bar, and a **View Alert** button is displayed. Click this button to find the corresponding alert in the **Network Alerts** list. If the View Alert button does not disappear after the issue has been solved, it can be concluded that the device has more than one issue that needs to be resolved.

6.2.1 Sorting order in Device List

The device names in the Device List are sorted in alphabetic order. If devices physically share the same location - for instance, they are situated in the same building, room or floor - then Network Docent is able to cluster these devices in the Device List, see figure 6.2.

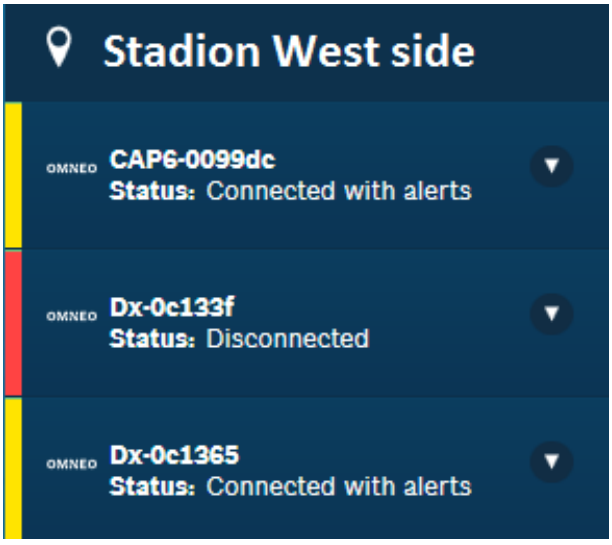


Figure 6.2: Devices that have been assigned the same location, are listed alphabetically under the name of their location

6.2.2 Locations

Depending on the extent of the network, the Device List can be a long list. By using **Locations** the list can be segmented. See also *Add locations, page 28* about how to add and assign locations to devices in Network Docent .
If locations have been assigned, the Device List will show these locations in alphabetic order, directly followed by their devices, also in alphabetical order. Devices that have no location assigned are displayed on top of the Device List, for instance:

DeviceA_without_location

DeviceB_without_location

etc.

RoomA

DeviceA in RoomA

DeviceB in RoomA

DeviceC in RoomA

RoomB

DeviceA in RoomB

DeviceB in RoomB

etc.

Location names are not clickable.

6.2.3 Add locations

Locations can be added following this procedure:

1. Open the **Device List**.
2. Click the green button marked **+ Add locations for devices**.
3. A dialog is displayed, showing a list of all devices followed by the names of their locations or an <unassigned> notice.

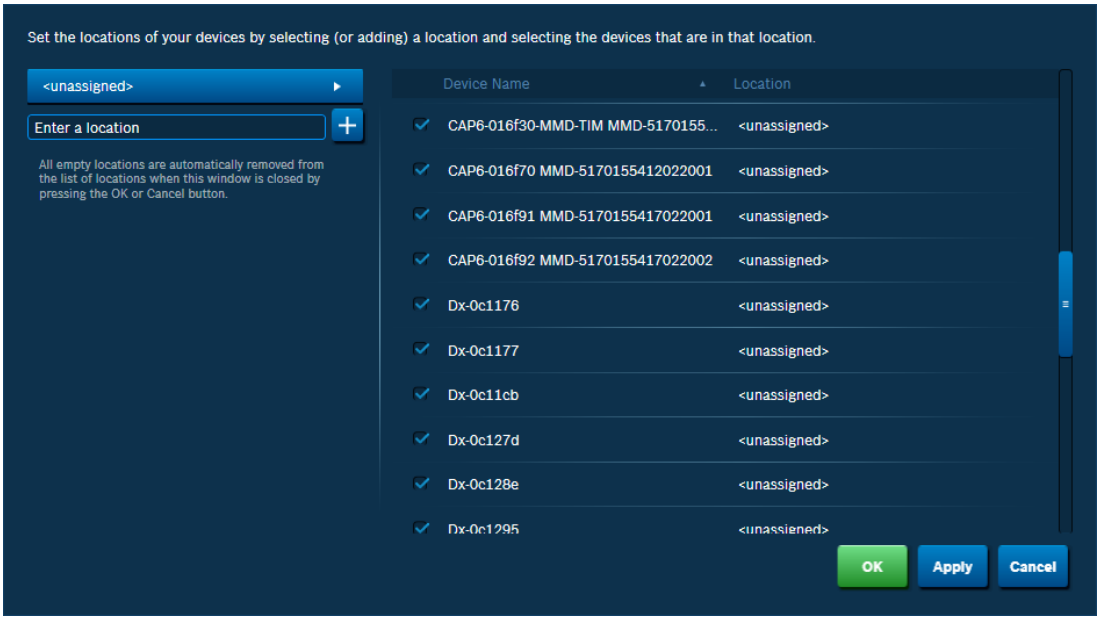
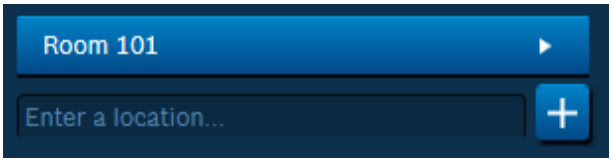


Figure 6.3: Set locations

4. Type the name of the new location in the text box in the left pane of the dialog.

5. Click the Plus button. The new name is now added to the **Location names list**.



6. Open the **Location names list** and hover the mouse over the location names; select one of the location names and click. The **Location names** list closes.

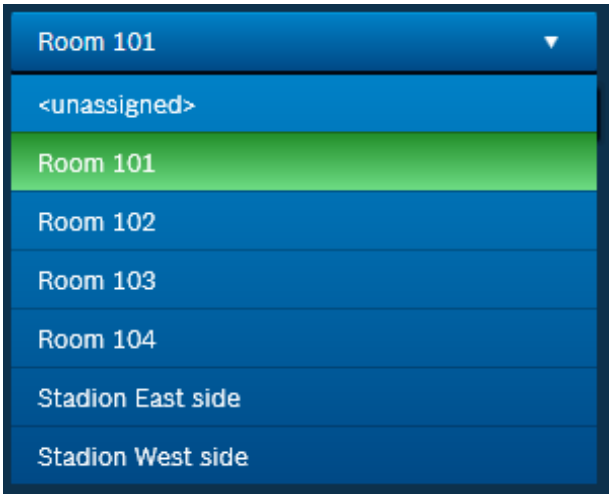


Figure 6.4: Example of Location names list

7. Now assign the selected location to one or more devices: in the right pane click all checkboxes of the devices, that are located in the selected location. Click the **Apply** button.

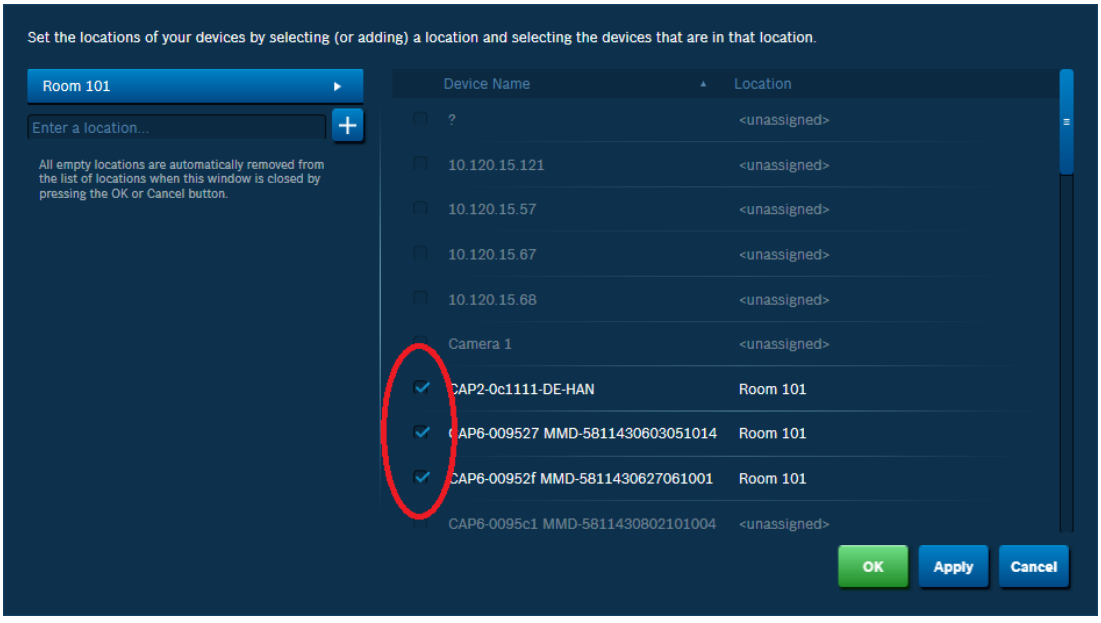


Figure 6.5: Three devices are now assigned to Room 101

8. Repeat these steps until all necessary locations have been defined and assigned. Click **OK**.
9. It is advised to store the locations and assignments by pressing hotkey **Ctrl + S** (Save).

Notice!
All defined and assigned locations will be stored after saving the application, for instance via **Menu > Save**.

Notice!
Location names that are not assigned to one or more devices, will automatically be removed from the **Location names list** after closing the add locations dialog.

6.2.4 Change locations

If devices are physically moved to another location, they have to be assigned a new location. Follow these steps:

1. Open the **Device List**.
2. Click the green button marked **+ Add locations for devices**.
3. If necessary, add a new location name to the **Location names list** (see *Add locations, page 28*).
4. Open the **Location names list** and select the appropriate location.
5. Now assign this location to one or more devices: in the right pane click all checkboxes of the devices that are moved to the selected location. Click the **Apply** button.
6. Repeat these steps for other devices that change location. Click **OK**.
7. Store the changes by pressing hotkey **Ctrl + S** (Save).

6.3 Device Alerts

The **Device Alerts** list is a copy of the Device List, and has the following differences:

– Only devices with issues are shown.
– The list is segmented into one or more issues, each followed by the device(s) that have the issue.
– If devices have multiple issues, they are shown more than once, in every alert segment that applies.
– If devices have multiple issues, and have a location name assigned, this location name will be shown in every alert segment that applies.

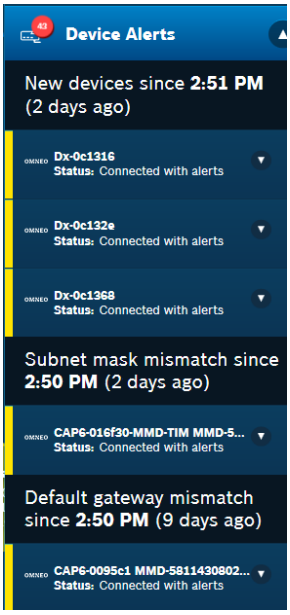


Figure 6.6: This Device Alerts list is segmented into three issues, each followed by the device(s) having the specific issue(s)

6.4 Network Alerts

All actual issues in the network are shown in the Network Alerts list, and categorized into seven alerts. If multiple devices have the same issue, they share *one* alert in the Network Alerts list. For details on each of the alerts, see also *Troubleshooting, page 43*, Troubleshooting.

- **Detected x new device(s)**
  New device(s) have been connected to the network.
- **Lost x device(s) and y connection(s) on z network(s)**
  Device(s) that were previously connected to the network are now disconnected.
- **No connection can be made to x device(s) on y network(s)**
  Docent is not able to connect to a newly detected device(s).
- **Duplicate IP address x.x.x.x found on y devices**
  Two or more devices with the same IP address have been found. This could be because duplicate static IP addresses have been set manually, or two DHCP servers may have distributed two or more identical IP addresses, or another reason may have caused this.
- **Detected default gateway x.x.x.x while expecting default gateway y.y.y.y**
  Devices with suspicious default gateways or another gateway mismatch are found. Network Docent uses its own default gateway and subnet mask as a reference; in case the PC has a wrong gateway and/or subnet mask, it will report all devices as having an issue.

Notice!
For the exact time and date, on which an alert was created, snoozed and/or approved, check the Events Log (see also *Events log, page 33*).

After clicking an alert all applicable node-symbols in the network visualization will be highlighted, and three buttons will show up, allowing you to take action on that specific alert:

– **Approve** - The alert is accepted as being an okay network situation. For instance: if the scan found x new devices, then these will be shown as yellow nodes in the visualization, and a network alert will be generated: 'Detected x new devices'. Check all x devices, then click the **Approve** button: the alert is removed and - if no other issues apply - the nodes change from yellow into green.
  Each time after clicking **Approve**, a small dialog is displayed, asking you to comment the approval (optional). This approval comment can later be found in the Events Log.

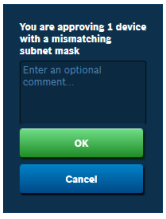


Figure 6.7: The optional approval comment that you type after your approval will appear in the Events Log

– **Troubleshoot** - The alert is explained in a help text that will help you solve the issue. For better readability, click the green **Expand** button on the upper right corner of the Help pane. See also *Troubleshooting, page 43*.
– **Snooze -** The alert is placed to the bottom of the list of active alerts, to be taken care of at a later time or date. The alert is marked with a snooze sign:

Postponements are useful if the alert has a low priority or if the error is due to changes that are knowingly being made on the network (such as adding, removing, or replacing devices). You can postpone for 1 hour or 1 day.

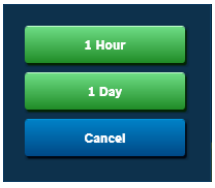


Figure 6.8: After clicking the Snooze button, you are asked for how long you want to postpone your action

6.4.1 Sorting order in Network Alerts list

Alerts in the Network Alerts list are sorted based on time: recent alerts are listed first and older alerts are at the bottom of the list. It the Network Alerts list contains snoozed alerts, then these are placed at the bottom of the list, again sorted on time. Example:
Alerts
alert 1, most recent creation date and time
alert 2
...
alert x, oldest creation date and time
Snoozed alerts
snoozed alert 1, most recent creation date and time
snoozed alert 2
...
snoozed alert x, oldest creation date and time

6.5 Events log

The Events Log provides a chronologic overview of events that occurred in the network. All events (and errors) are listed, including all approved events. Two details are listed for each event: severity (Warning, Error or Critical) and a short Event Description.

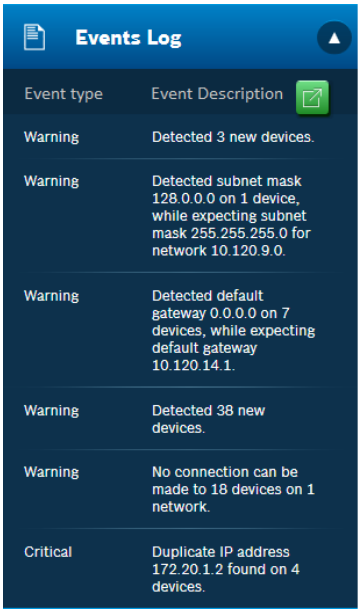


Figure 6.9: Example of the Events Log, showing description and severity on each event

More details on the events can be obtained by clicking the green **Expand the view** button on the upper right corner of the Events Log pane.

The complete Events Log contents is then opened in the center pane of the screen. Another way is to click one of the events in the Events Log: again all contents is opened in the middle pane, but now the clicked-on event is highlighted and expanded.

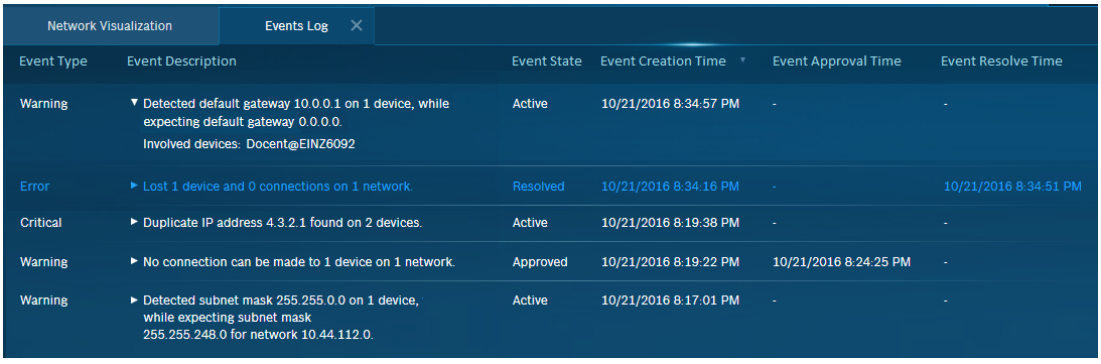


Figure 6.10: The expanded Events Log provides exact date and time stamps on each event

The center pane shows additional information on the event: Event State (Active, Resolved, or Approved), Event Creation Time, and Event Approval Time (if applicable), and Event Resolve Time (if applicable). Sort the list by clicking once, twice or three times on the titles in the header of the list. The first two clicks will toggle the sorting order between ascending and descending; the sorting order is indicated by the vertical arrow next to the column title. The third click will disable sorting (arrow disappears). It is possible to sort on multiple columns simultaneously, e.g. event state and event creation time.

The small arrow in front of each Event Description hides a list of involved devices and – if applicable – approval comments (see also *Menu, page 36*). Click one of the arrows, or the Event Description itself, to unroll a similar list as is shown in the first lines of figure 6.10. Return to the network visualization by clicking the cross in the **Events Log** tab on top of the center pane.

Notice!
The Events Log is stored and digitally encrypted in the snapshot file.

6.6 Help

Clicking **Help** opens a list of **Top Solutions**. Click on one of the Top Solutions to reveal a list of articles on that specific solution. Click again to hide the articles. The articles originate from Network Docent's built-in Knowledge Base (see also *Knowledge base, page 43*) and will help you solve issues.
Each article starts with a title. For instance, click the first topic in the Help pane: **How to resolve missing devices** (see figure 6.11). This will show all corresponding articles, for instance:

- Disconnected network cable
- Missing mains or unpowered device
- Incompatible IP configuration
- Missing OMNEO devices
- Missing SNMP devices
- OMNEO Security
- SNMP Security
- Incorrect Local PC interface configuration
- VLAN mismatch

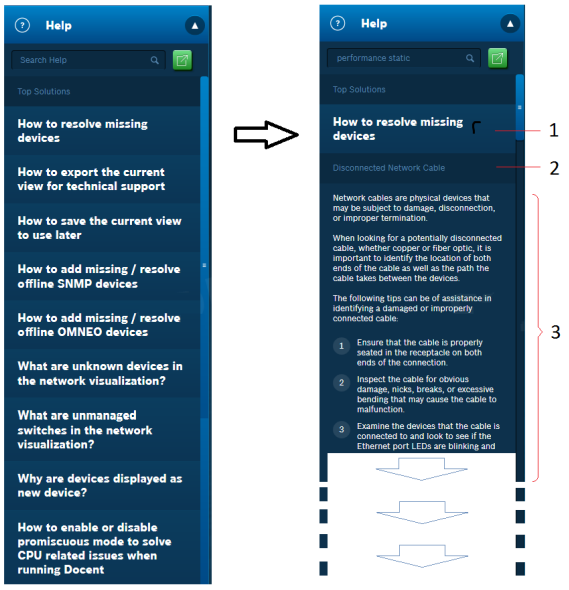


Figure 6.11: List of 'Top Solutions' – clicking one of the solutions (1) shows a list of corresponding articles, each article starts with a title (2), followed by text (3)

The Search Help function allows you to perform a search in the knowledge base. By typing the first character(s), a list of suggested keywords starting with that/those letter(s) will be shown. Select the keyword from the list or type it manually. If needed, add more keywords by first typing a space and then selecting or typing additional keyword(s). For instance, in figure 6.12 a search is performed using the keywords 'performance static'.
Click the magnifying glass icon to start the search. The results list will show a selection of the Top Solutions; click one of these Top Solutions to open all corresponding articles. One or more of these articles will contain the keyword(s).

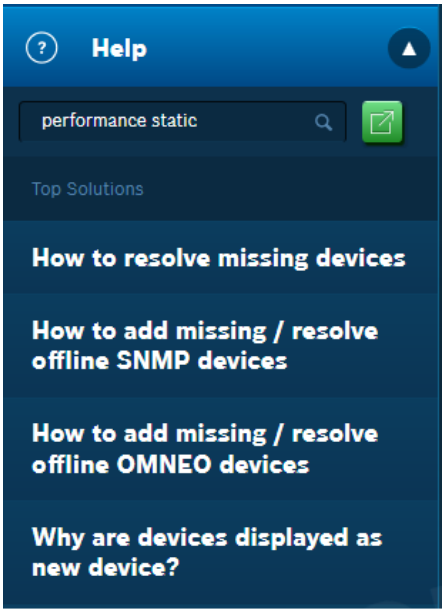


Figure 6.12: Search on one or more keywords

Notice!
Search actions on other words than the suggested keywords will produce an empty results list

To enhance readability, click the green **Expand the view** button in the Help pane. This will open the help text from the pane in a new **Help** tab in the center pane of the screen. Close the expanded help text by clicking the cross in the Help tab.

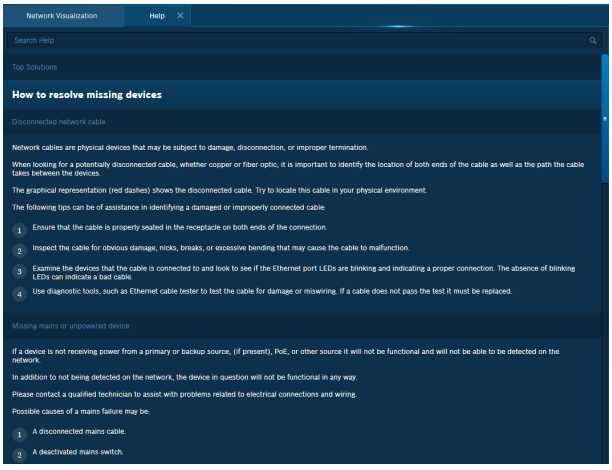


Figure 6.13: Help in Expanded view

6.7 Menu

The **Menu** button is situated on the upper left corner of the Network Docent window. Clicking it will open Network Docent's menu. This chapter will describe all menu options.

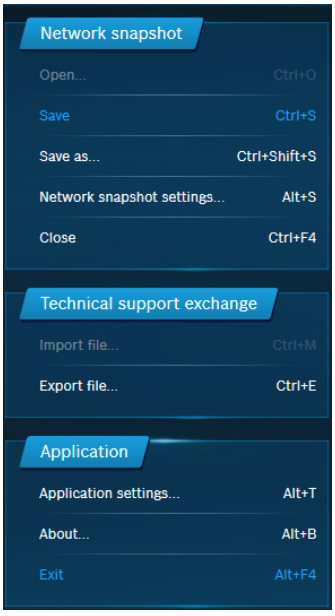


Figure 6.14: Network Docent's menu

6.7.1 Close and Exit

There are two ways to stop the current Network Docent session:

- Are you finished monitoring and diagnosing your network with Network Docent, click **Menu > Exit**, or press hotkey **Alt + F4** instead.
- Do you want to start a new scanning session or open a snapshot file, click **Menu > Close**, or press hotkey **Ctrl + F4** instead.

If you made any changes in the network visualization, the locations and/or the application settings, then:

- The changes will be automatically saved, if the option **Automatically save network snapshot when closing application** is switched on. This option is located at **Menu > Application Settings** (see also *Application Settings, page 41*).
- You will be prompted to save these changes. Click **Save** (see also *Save and open network snapshot, page 36*) or **Don't save**.

6.7.2 Save and open network snapshot

1. The purpose of saving the network visualization and configuration is to obtain a reference for later troubleshooting uses. Saving the network visualization and configuration means saving a 'snapshot' of the situation at a certain moment; the next moment connections and settings may have changed. The snapshot is stored in a snapshot file.
2. Click **Menu > Save as**.
3. The suggested filename format has the current date and time in it:
   `NetworkSnapshot_2099-12-31_12-00`
4. Accept this name or type another name (spaces are allowed). Click **Save**.

Notice!
If changes are made to the network after the snapshot has been made, and you want to update the snapshot file, just click **Menu > Save**, or press hotkey **Ctrl + S**.

To open a previously saved snapshot:
1. Close the current network visualization: click **Menu > Close**. Or press hotkey **Ctrl + F4**.
2. Optionally save the current network visualization. Warning: type or use another name different from the filename of the snapshot you want to open!
3. Open the snapshot file: click **Menu > Open**. Or press hotkey **Ctrl + O**.
4. Select the snapshot filename and click **Open**.

Notice!
The snapshot filename is displayed in the upper left corner of the network visualization. To change this name, click **Menu > Save** as, type the new name, and click **Save**.

Notice!
A snapshot file may contain passwords and other security parameters. If you do not want any secure content to be stored, then use Docent's Import/Export functionality (see also *Technical support exchange, import, export, page 39*).

Notice!
Snapshots are saved in the current user's personal Windows profile and cannot be interchanged between other computers and users. It you want to interchange, use Docent's Import/Export functionality (see also *Technical support exchange, import, export, page 39*).

Notice!
Open multiple files simultaneously by starting Network Docent multiple times. This can be useful to compare system states, e.g. last week's snapshot and yesterday's snapshot.

6.7.3 Network snapshot settings

Network Docent supports two control protocols for IP networks: OCA and SNMP. Both protocols feature a security mechanism that protects the network equipment from any unwanted communications and from being scanned by unauthorized systems. In order for Network Docent to communicate securely with these devices and retrieve their status information, the proper credentials (like username/passphrase) must be provided. Without these credentials Network Docent's network visualization will display the devices as 'Disconnected'.

OCA Settings
For Bosch OMNEO and other OCA devices that are configured for secure communications, follow these steps:
1. Click **Menu > Network snapshot settings**. Or press hotkey **Alt + S**.

2. Open the tab **OCA Settings**.
3. Fill in the username and passphrase, as have been defined for the Bosch OMNEO system.
4. Click **Add**. The provided information is added to the list on top of the tab.
5. Repeat these steps for any other OCA audio systems in the network.
6. Click **OK** and return to the network visualization.

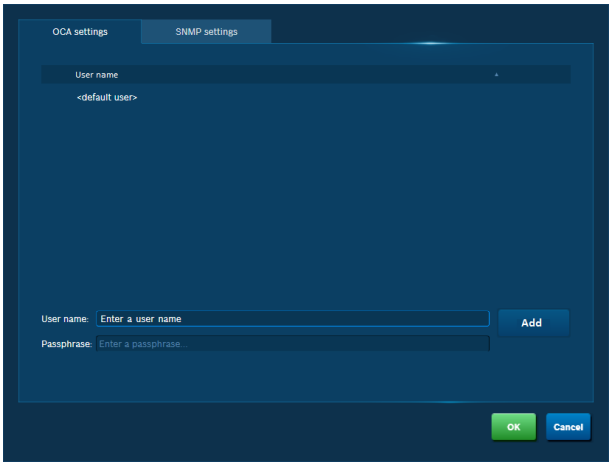


Figure 6.15: Adding credentials for Bosch OMNEO and other OCA devices

SNMP Settings

For third party devices with SNMP support that are configured for secure communications, follow these steps:

1. Click **Menu > Network** snapshot settings. Or press hotkey **Alt + S**.
2. Open the tab **SNMP Settings**.
3. Fill in all credentials for the first relevant SNMP device (host):
   Host IP address, for instance, 192.168.0.1
   Port number, for instance, 161
   SNMP Version, for instance, v1
4. Click **Add**. The provided information is added to the list on top of the tab.
5. Repeat these steps for all relevant devices.
6. Click **OK** and return to the network visualization.

Notice!
Use the default Host IP address 0.0.0.0 to set the credentials for all SNMP devices at once.

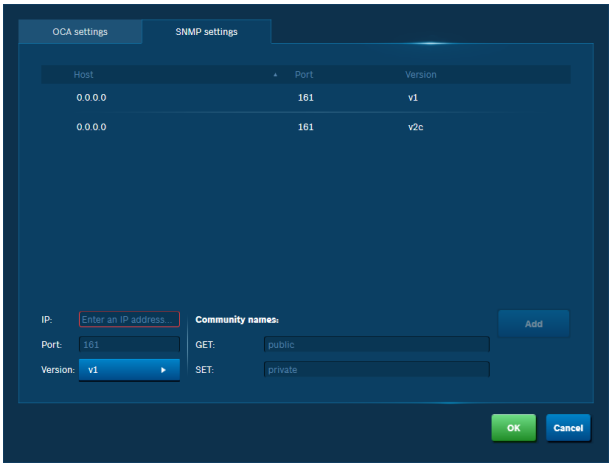


Figure 6.16: Setting credentials for SNMP devices

6.7.4 Technical support exchange, import, export

The purpose of exporting is to save a snapshot as a 'Network export file', that contains the current network visualization and all location names that may have been added to devices.

1. Click **Menu > Export** file or press hotkey **Ctrl + E**.
2. The suggested filename format has the current date and time in it:
   `NetworkSnapshot_2099-12-31_12-00.docentxml`
3. Accept this name or type another name (spaces are allowed).
4. In the left pane of the dialog, select the right path for the file to be saved in.
5. Click **Export**.

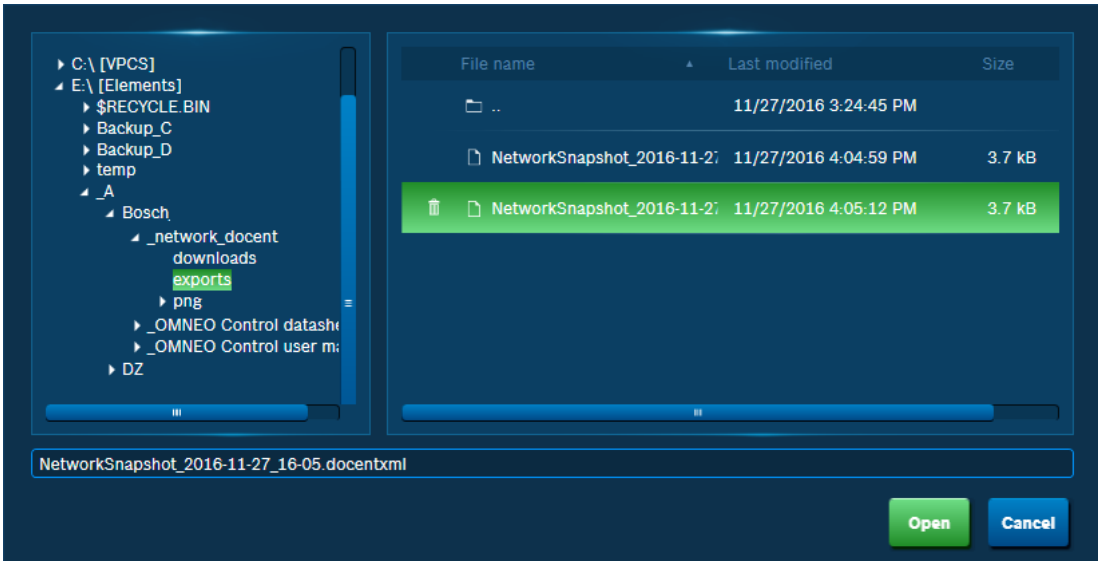


Figure 6.17: Choose the path you want to store the Network export file in

If changes were made to the network after the export file was generated, and you want to update or delete the Network export file, click **Menu > Export file**, and select the filename of the export file:

– If you want to delete the file, click the small dustbin icon in the green bar and confirm the warning by clicking **Yes**.
– If you want to update the file, click **Export**. A dialog appears with a warning: **Are you sure you want to overwrite this Network export file?** Click **Yes**.

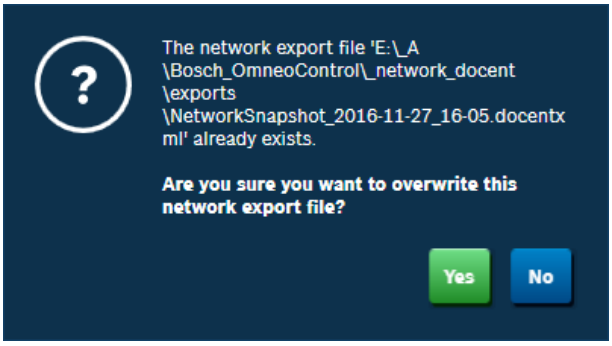


Figure 6.18: Overwriting the Network export file

To import a previously exported snapshot:

1. Close the current network visualization: click **Menu > Close**. Or press hotkey **Ctrl + F4**.
2. Optionally save the current network visualization.
3. Open the Network export file: click **Menu > Import....** Or press hotkey **Ctrl + M**.
4. Select the path in which the file is stored.
5. Select the filename and click **Open** (or double-click it).

Notice!
Another way of opening a Network export file is by double-clicking the filename in Windows Explorer.

The default filename extension of a Network export file is .docentxml. Use Windows Explorer to copy the Network export file to a USB-stick or other media, for transfer to a technician or technical support for further analysis and troubleshooting uses. The file can be opened on any machine that has the Network Docent application installed. For this reason - in contrast to a snapshot file created with Network Docent's **Save** function - secure information - like pass phrases for OCA and SNMP - is not present in the Network export file to avoid misuse of this information.
The differences between a Snapshot file and a Network export file are summarized in the table below:

Property	Snapshot file	Network export file
Secure information included	yes	no
Folder in which file is stored	fixed	user selectable
Filename extension	.sdocentxml	.docentxml
Used for technical support	No	Yes
Can be opened on	PC the snapshot is created on	

Differences between Snapshot file and Network export file

Notice!
A Network export file does not contain pass phrases and other security parameters. If you want to store any secure content, then use Docent's Save/Open functionality (see also *Save and open network snapshot, page 36*).

Notice!
Only exported snapshot files with a .docentxml filename extension can be shared across computer systems.

Notice!
Network Docent is backwards compatible to export files created by older versions. Forward compatibility is not supported. If you try to import such a Network export file, an error message will be displayed. Update your version of Network Docent. See also *Updating Network Docent, page 12*.

6.7.5 Application Settings

Network Docent has three settings for you to check.

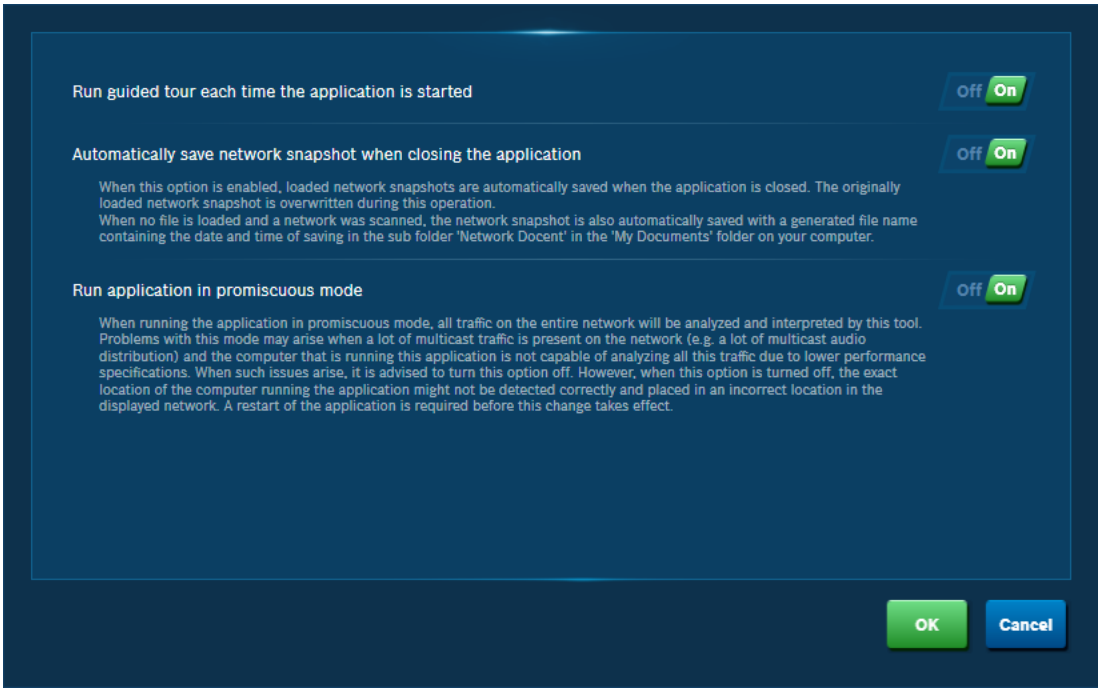


Figure 6.19: Application settings

Run guided tour each time the application is started
When enabled, this option will automatically welcome the user with a Guided Tour, each time Network Docent is started. The default setting for the **Run guided tour each time the application is started** option is **On**.

Automatically save network snapshot when closing application
When enabled, this option will automatically save a snapshot of the current network visualization, each time the application is closed. The last saved network snapshot file will automatically be overwritten. If the current network visualization does not yet carry a Network snapshot name, Network Docent will generate a filename, containing the current date and time, and using this format:
`NetworkSnapshot_2099-12-31_12-00.sdocentxml`
The default setting for the **Automatically save network snapshot when closing application** option is **Off**.

Run application in promiscuous mode

When promiscuous mode in Ethernet local area networks (LANs) is enabled, the network interface (NIC) in your PC 'listens' to all data that is sent over the network; the data can be received by any PC. Promiscuous mode is the preferred mode to monitor network activity. That is why the default setting for this option is **On**.

Setting this option to **Off** will cause Network Docent to run in non-promiscuous mode. When the network interface of a device is in non-promiscuous mode it only receives data which is explicitly addressed to this device. In non-promiscuous mode the PC will get much less network traffic, but Network Docent cannot reliably detect its own position on the network.

Notice!

Not all network chipsets support promiscuous mode. This may cause Network Docent to display an error message: 'The Network Docent application is unable to set the promiscuous mode to the neighbor discovery driver. The location of this computer in the network might not be accurately detected and shown. A reboot might resolve this issue.'

Notice!

Disabling promiscuous mode does change the network visualization and can cause a disconnect alert for the PC running Network Docent.

7 Troubleshooting

7.1 Knowledge base

Network Docent has a built-in knowledge base which contains several dozens of articles. These articles contain useful information, which will help you solve issues, when you are troubleshooting and diagnosing a network's infrastructure and devices. You get access to these articles via Network Docent's **Help** function (see also *Help, page 34*) and via **Alerts**.

7.2 Alerts

During its scanning operations Network Docent may encounter issues in the network. Each issue will result in an alert in the Network Alerts list and a color- and status-change in the network visualization:

– Device-level zoom: each device is represented by a node-symbol that will show the device name and its status. If this status points to an alert, the node-symbol will be red (critical alert) or yellow (warning alert).
– Lower zoom-levels: the network visualization groups devices in large node-symbols. If one or more of the devices in a group carry an alert, then the group's node-symbol mentions the total number of devices having an alert, and is colored red or yellow.

Notice!
If a device has two or more issues, both are listed in the Alert List. The most critical alert is shown in the network visualization. After this issue is solved, the next alert is shown.

Alerts and their color-codings are also made visible in the right and left panes of the screen:

– Device List	The Device List shows details of the selected device, including red **View Alert** buttons for devices having an issue.
– Device Alerts list	Same as Device List, but only devices that have a **View Alert** button are shown.
– Network Alerts list	The Network Alerts list shows the alert, including **Troubleshoot**, **Approve** and **Snooze** buttons. The list groups all equivalent alerts into a smaller number of alerts, mentioning the number of devices giving that alert. For instance: 'Detected 8 new devices'.

7.3 General troubleshooting procedure

Troubleshooting and diagnosing the network usually starts from an alert in the Network Alerts list. From here you are linked to one or more corresponding articles in the knowledge base. These articles provide detailed information, helping you to solve the issue(s) that caused the alert(s). Follow these six steps:

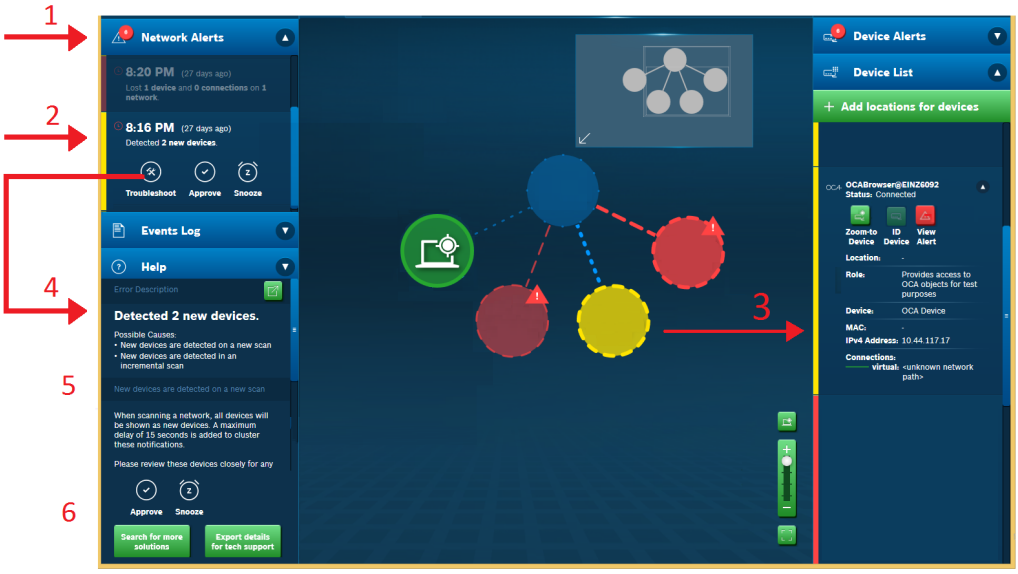


Figure 7.1: The general troubleshooting procedure takes six steps (step numbers are explained in the text)

1. Open the **Network Alerts** list. Each alert is preceded by a time/date stamp, indicating the moment the alert appeared for the first time, for instance:

8:16 PM (27 days ago)
Detected **1 new device**.

Identical alerts of multiple devices are grouped together into one or more group alerts in the **Network Alerts** list, mentioning the total number of devices, for instance:

8:16 PM (27 days ago)
Detected **2 new devices**.

2. Click the alert in the **Network Alerts** list to highlight all involved devices in the network visualization. These devices might be spread out all over the network, so - if necessary - shift the network visualization to locate them all.
3. Optional: additional information about the highlighted devices can be found in the Device List, by clicking a specific device.
4. Click the **Troubleshoot** button.
5. The **Help** pane is opened, showing a short **Error Description** and a list of possible causes, followed by applicable article(s) derived from the knowledge base.
6. You now have the following options:

– Try to solve the issue, using the clues given in the article(s). Check the Network Alerts list and the network visualization: if the issue has been solved, the alert will be removed and the node-symbol(s) of the devices - having that specific issue - will change. See notice.
– Postpone solving the issue to a later date: click **Snooze**. In the Network Alerts list the issue is moved to the bottom of the list, and marked with a snooze-icon (see figure).
– Accept the issue and click **Approve**. If the device(s) have no other issues, the node-symbol in the network visualization will change. After clicking **Approve**, a small dialog is displayed, asking you to comment the approval (optional). This comment will be registered in the Events Log.

– Consult additional knowledge base articles by clicking **Search for more solutions**.
– Create a snapshot of your current network situation, and store it in a Network Export file. Present the snapshot file to technical support. See also *Technical support exchange, import, export, page 39*.

If you want to learn how to take these steps in a real network environment, see also *General troubleshooting procedure - example, page 45*.

Notice!
The network visualization will be updated continuously and immediately after each change in the network. Updating alerts in the Network Alerts list may take up to 15 seconds after each change.

7.3.1 General troubleshooting procedure - example

Case: After Network Docent Network Docent has finished its scanning operation, ten devices in your network appear to have generated a **Gateway mismatch** alert. Follow the general troubleshooting procedure (the six steps correspond to figure 7.1):

1. Open the **Network Alert** list, see figure.

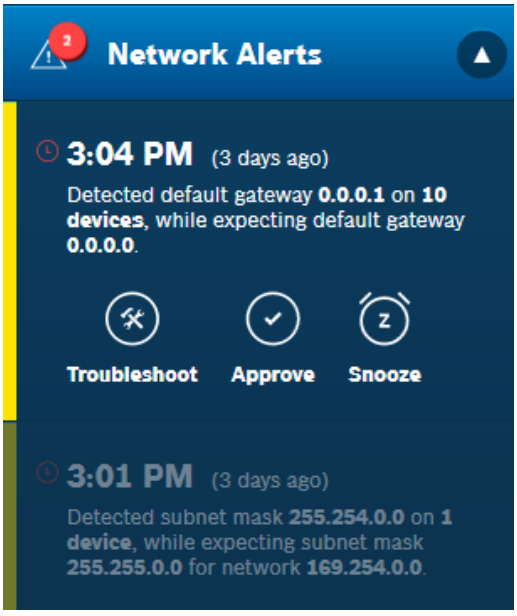


Figure 7.2: Multiple identical alerts are grouped into one

2. Click the alert to highlight all involved devices in the network visualization.
3. Optional: additional information about highlighted devices can be found in the Device List, by clicking the corresponding mode-symbols in the network visualization.
4. Click the **Troubleshoot** button.
5. The Help pane is opened, showing the possible cause (Default gateway mismatch), plus one or more articles from the knowledge base. Read the article(s), they may give you clues about how to solve the issue.
6. You now have the following options:
   – Review the devices for their expected and detected default gateways.
   – Correct the configuration, in case the detected default gateway was misconfigured.
   – Click **Snooze** and postpone the issue. In the Network Alerts list the issue is moved to the bottom of the list, and is marked with a snooze-icon.

- Click **Approve** and accept the inconsistency. The detected default gateway will be added to the whitelist of default gateways, so no further alerts will be generated for the detected default gateway.
- Consult other knowledge base articles by clicking **Search for more solutions**.
- Click **Menu > Export...** and create a Network export file for technical support. See also *Technical support exchange, import, export, page 39*.

7.3.2 Troubleshooting from network visualization

As stated, troubleshooting and diagnosing the network usually starts from an alert in the Network Alerts list, and does not start from a device's node-symbol in the network visualization. For instance, if 20 devices have a lost connection, this is probably caused by one loose cable, or by one switch being powered off. The alert in the Network List groups all 20 devices in one alert that you can troubleshoot at once. The 20 devices in the network visualization on the other hand, each have their individual red or yellow node-symbol, which would all have to be troubleshot one by one. However, it can be done and will take eight steps, as is depicted in figure 7.3. The last of these steps end in the same way as the general troubleshooting procedure:

1. Set the zoom slider to device-level zoom.
2. Click a node-symbol that is containing the alert.
3. Details on the corresponding device are displayed in the **Device List**.
4. Click the red **View Alert** button in the Device List.
5. Identical alerts of multiple devices may be grouped together into one or more group alerts in the **Network Alerts** list. Click the group alert to highlight the specific devices in the network visualization, and to pinpoint the location of the error e.g. a switch to which all of these devices are connected.
6. Click the **Troubleshoot** button.
7. The Help pane is opened. Read the **Error Description** and the possible causes
8. The articles give you hints about how to solve the issue.

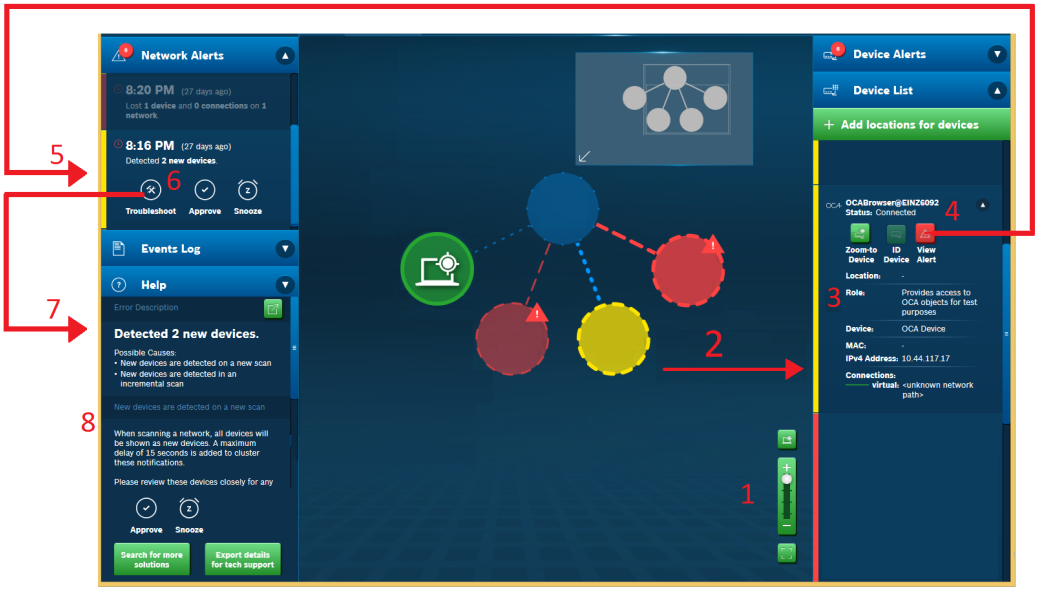


Figure 7.3: Eight steps of troubleshooting starting from the network visualization (step numbers are explained in the text)

7.4 Details on Network Alerts

All actual issues in the network are shown in the Network Alerts list, and categorized into seven alerts. All seven alerts are described in this chapter.

7.4.1 Lost x device(s) and y connection(s) on z network(s)

Device(s) that were previously connected to the network now appear to have been removed from the network. The time stamp in the Network Alerts list mentions the first time, the connection was lost. For instance:

2:50 PM
Lost 2 devices and 3 connections on 2 networks

Follow the general troubleshooting procedure.
The Help pane shows a list of possible causes and solutions. Some possible causes are:

- Disconnected network cable
- Missing power, check mains cord or power supply
- Incompatible IP configuration, check device network settings
- Missing OMNEO devices
- Missing SNMP devices
- OMNEO Security
- SNMP Security
- Local PC network configuration
- VLAN mismatch
- etc.

Approving this 'Disconnected' alert will remove the node-symbol from the network visualization.

Notice!
Managed switches allow the configuration of Virtual LANs or VLANs. This means that multiple 'LANs' can exist in a single switch. Please note that devices that are part of these VLANs may show up as Disconnected devices, because they cannot communicate to each other directly without the help of a router.

7.4.2 No connection can be made to x device(s) on y network(s)

Certain conditions may inhibit Network Docent Network Docent to connect to devices. Two of these conditions are:

- Invalid username and/or passphrases for SNMP and OCA. See also *Network snapshot settings, page 37* about credentials.
- The device has reached the maximum number of network connections it can make.

As with the 'Lost devices' alert, these conditions will (also) generate red node-symbols with a **Disconnected** status in the network visualization, while the Network Alerts list will show an alert like:

2:50 PM
No connection can be made to **18 devices** on **1 network**

Follow the general troubleshooting procedure.
The Help pane shows a list of possible causes and solutions. Some possible causes are:
- Possible AES70 compatible controller conflict
- Incompatible IP configuration
- SNMP Security
- Missing SNMP devices
- OMNEO Security
- etc.

Approving this 'Disconnected' alert will not remove the node-symbol from the network visualization, since Docent is certain it is present.

7.4.3 Detected x new device(s)

The **New Device** alert is a very common alert. After Network Docent has finished its first scanning operation, or after you have added device(s) to the network, one or more **New Device** alerts will be generated. For instance:

8:16 PM (27 days ago)
Detected **2 new devices**.

New devices deserve your attention, because they influence the network's performance and security. For instance, unexpected rogue devices and other unwanted network nodes may behave badly by consuming excessive bandwidth or exposing audio and control traffic.
- Review the new device or devices one by one, not only in Network Docent but also physically in the network. If the alert points to more than one device, you can find information about each individual device in the **Device List** or **Device Alerts** list.
- Remove unwanted devices from the network. Check the network visualization: removed devices should be indicated as 'Disconnected' and - after approving this alert – will be removed from the network visualization.
- Approve the alert: all new devices will be accepted as okay. If no other alerts apply, their node-symbols will turn to green.
- Follow the general troubleshooting procedure for a detailed description of the steps to take.

7.4.4 Duplicate IP address x.x.x.x found on y devices

A **Duplicate IP address** alert is generated, when Network Docent detects two or more devices, which both report the same IP address. Duplicate IP addresses cause serious errors in your network: audio streams might stop playing unexpectedly, control of devices will become unreliable etc. The alert in the Network Alerts list may look like this:

2:50 PM
Duplicate IP address

Follow the general troubleshooting procedure.
The Help pane shows a list of possible causes and solutions, like:
- Devices have duplicate static IP address.
- Make sure all devices have a unique IP address by changing IP addresses of each device with a duplicate. Consult the device's manual for instructions on how to do this. Remark: using static IP addresses is not preferred, because they can easily lead to issues as described here. Instead, it is recommended to use dynamic IP addresses.
- DHCP servers may have distributed two identical IP addresses.
- This can happen, when multiple DHCP servers in the network are configured for stand-alone mode. To avoid issues, make sure the assigned IP ranges for each of the DHCP servers don't overlap. When configured in redundant mode, make sure the two DHCP servers are able to communicate with each other to exchange their information about redundancy or load balancing parameters. Check if one is reporting as a master and the other one is reporting as a slave. Consult the manual of the DHCP servers for instructions.
- Follow the general troubleshooting procedure for more information on this issue.

Notice!
For locating devices with duplicate IP address in the network visualization, do not search for these addresses using the Search function (only one device will be found). Instead, click the appropriate alert in the Network Alerts list: the devices sharing the same IP-address will be highlighted.

7.4.5 Detected default gateway x.x.x.x while expecting default gateway y.y.y.y

Network Docent detected a mismatch of the reported default gateway of an endpoint device and the default gateway of the PC running the Network Docent application. Generally, a network has a single default gateway used by all devices to access other subnets. However, multiple default gateways are also possible and might be useful under certain conditions. The **Network Alerts** list may report the alert like this:

9:37 AM
Detected default gateway **10.0.0.0** on **1 device**,
while expecting default gateway **0.0.0.0**

- Follow the general troubleshooting procedure.
- The Help pane shows a list of possible causes and solutions. Possible solutions are:
- Review the reported devices for their expected and detected default gateway.
- Approve the alert to accept the detected inconsistency. The detected default gateway will be added to the whitelist of default gateways (no further alerts will be generated for the detected default gateway).
- Correct the configuration in case the detected default gateway is a misconfiguration.

– Other solutions given by the application.

7.4.6 Detected subnet mask x.x.x.x on z device(s), while expecting subnet mask y.y.y.y for network z.z.z.z

The network may contain one or more devices with suspicious subnet masks. Network Docent detected a mismatch of the reported subnet mask of an endpoint device and the subnet mask that is set on the PC which is running Network Docent, and is on the same network. This will inhibit devices communicating to other devices.
Follow the general troubleshooting procedure. The Network Alerts list may report the alert like this:

8:17 PM
Detected subnet mask **255.246.0.0** on **1 device**, while expecting subnet mask **255.255.246.0** for network **10.44.111.0**

Follow the general troubleshooting procedure.
The Help pane shows a list of possible causes and solutions. Possible solutions are:
– Review the reported devices with their expected and detected subnet mask.
– Correct the configuration in case the detected subnet mask is a misconfiguration. When a DHCP server is used, this configuration needs to be adapted in the DHCP server configuration. For static IP refer to the manual of the device.
– **Approve** the alert to accept the detected inconsistency, the detected subnet mask will be added to the whitelist of subnet mask for the reported devices.
– Other solutions given by the application

7.5 Notices

7.5.1 What are 'Managed switches' and 'Unmanaged switches' in the network visualization ?

An unmanaged switch is a simple networking device that connects other devices to a computer network. It is a plug and play device, without any special features, without configuration settings, and without LLDP and SNMP. Unmanaged switches are often used in a small office/home office environment, because they are typically the least expensive switches. Managed switches are more expensive and support a lot more functionality, including LLDP and SNMP support.
– LLDP and SNMP enabled switches and bridges are detected, and fully supported by Network Docent.

Network Docent will show a blue node-symbol with an **Unmanaged switch** notice in the network visualization if:
– Multiple devices are detected, all sharing the same network segment. Most likely, an unmanaged switch is connected between these devices.

– The device was still found on a port, although the device has been removed. This usually is a temporary situation that will resolve itself automatically within 90 seconds. During this short period of time, the 'Unmanaged switch' node-symbol is shown.
– Managed switches with both LLDP and SNMP disabled are considered unmanaged switches.

Notice!
Managed switches, of which ports are connected to other switches without SNMP and/or LLDP functionality, or which have their SNMP functionality disabled, may be detected by Network Docent as 'unmanaged switches'.

7.5.2 What is an 'Unknown Network Path' in the network visualization?

Devices found on the network are connected to the network by a physical (or wireless) network connection. The network visualization will show a blue node-symbol with an **Unknown Network Path** notice in case the physical location of the device cannot be determined. This occurs under the following conditions:
– Network device has no LLDP available, which makes it impossible to determine the exact device location.
– Device does support SNMP but no SNMP session could be established.

Because the device is beyond reach, Network Docent cannot provide information about the device. You could check one or more of the following, to help Network Docent gather more information:
– Make sure LLDP is enabled on all managed network devices.
– Make sure SNMP is enabled on all managed network devices and their credentials are well known within Network Docent.

7.5.3 What is an 'Unknown device' in the network visualization?

The network visualization will show a blue node-symbol with an **Unknown device** notice if:
– Network Docent detects an active port on a managed device, but the connected device does not provide any information.
– Because of the lack of information, the device is absent in the Device List. You could check one or more of the following, to enable Network Docent gather more information:
– Make sure LLDP is enabled on all managed network devices.
– Make sure SNMP is enabled on all managed network devices and their credentials are well known within Network Docent (see also *Network snapshot settings, page 37*).

7.6 Troubleshooting while building a new installation

Configuring a new network means connecting devices and cables. By doing this step by step, Network Docent Network Docent can be used to test each step before continuing to the next. Each step will result in either of these outcomes:

– Device is not detected by Network Docent
  Check the network, check the cables and its connections, check the device, check if the device is switched on. If the problem is resolved, you can add the next device.
– Device is detected by Network Docent
  The device is visible in the network visualization and in the device list. Optionally you may add a location to the device by clicking **Add locations for devices** in the Device List. Add the next device.

When the network is properly setup and running well, it is a good habit to save the network scan for future reference in a snapshot file. See also *Save and open network snapshot, page 36*.

7.7 Troubleshooting an existing installation with a snapshot

An existing installation may be operational for a long time, without any problems occurring, until suddenly issue(s) arise. Use Network Docent to evaluate the network, to identify any issues, by comparing the network's status with an earlier snapshot, taken when the network was working fine. To perform such a comparison a snapshot file has to be available, containing a previously stored network configuration and network scan. This is what you do:

1. Start Network Docent.
2. Click **Menu > Open** and open a previously stored snapshot, made when the network was running well.
3. Start scanning and study the new alerts. The alerts point out what changes have taken place in the network.
4. Try to resolve the causes of the alerts, and check if the alerts disappear. Allow Network Docent a few seconds to rescan the network, after each change you make. The network visualization is updated immediately, updating the Network Alerts list may take up to 15 seconds.

Notice!
Comparing a network visualization with a previously saved snapshot is not necessary, if Network Docent is constantly active and scanning your network. Check the Events Log to discover what went wrong.

8 Support

8.1 Customer service

Refer to product related information on: www.boschsecurity.com.
If a fault cannot be resolved, please contact your supplier or system integrator, or go directly to your Bosch representative.

8.2 Technical support exchange

When consulting technical support about issues and errors in your network, you may be asked to make a snapshot of your network and send it to them. See also *Technical support exchange, import, export, page 39* how to export a snapshot - containing your network configuration and settings - to a Network export file, that does not contain any secure information. Such a Network export file can be sent (by email) or handed over (by USB-stick) to technical support.

8.3 Troubleshooting the Network Docent application

If you encounter a problem while working with Network Docent, these resources may prove to be helpful:

- Consult the Troubleshooting table, see below.
- For troubleshooting network related issues concerning Bosch OMNEO products, see also the OMNEO Resource Guide.
- The Events Log may give you more information about the problem.

Error message	Occurrence	Solution
Network Docent failed to load the requested Network export file `<path/filename.docentxml>`	This error may occur after clicking **Menu > Import file...** in order to import a previous saved Network export file.	The current user does not have sufficient access rights to access the requested file. Please update the access rights (read/write) on the selected file and retry.
		The file requested to load is currently in use by another program. Close all other programs and retry loading the file. If this does not help, reboot your PC, and try again.
		The file requested to load is not found in the specified path. Make sure that the current user has the appropriate rights to access the requested file.
An unknown error occurred when loading the file.	This error may occur after clicking **Menu > Import file...** in order to import a previously saved Network export file.	Make sure you have the latest version of Network Docent installed. Please note that only *exported* files can be shared across computer systems.

The file requested to load has been created with a newer Network Docent version.	This error may occur after clicking **Menu > Import file...** in order to import a previously saved Network export file.	Please update your Network Docent version to the latest version and retry loading the file.
Network Docent failed to save the current Network export file in the requested location <path/filename>	This error may occur after clicking **Menu > Export file...** in order to create a Network export file.	The current user does not have sufficient access rights to access the requested file and/or path. Please update the access rights (read/write) on the selected file and path and retry.
		The current snapshot seems to contain invalid data and therefore cannot be saved. Please retry to save. In case the problem continues to occur, your snapshot is corrupted. A new network snapshot needs to be created.
		An unknown error occurred when saving the file. Make sure the file is not open in another application and that the current user has write access to the requested location.
Network Docent failed to load the requested network snapshot <filename>	This error may occur after clicking **Menu > Open** in order to open a previously saved snapshot.	The current user does not have sufficient access rights to access the requested file. Please update the access rights (read/write) on the selected file and retry.
		The file requested to load is currently in use by another program. Close all other programs and retry loading the file. If this does not help, reboot your PC, and try again.
		The file requested to load is created using the save method on a different machine. Snapshots that are saved are not transferable from machines. Use the

		export function on the original machine and load the generated Network export file on this machine.
Network Docent failed to save the requested network snapshot `<filename>`	This error may occur after clicking **Menu > Save** in order to save a snapshot.	The current user does not have sufficient access rights to access the requested file. Please update the access rights (read/write) on the selected file and retry.
		The current snapshot seems to contain invalid data and therefore cannot be saved. Please retry to save.
		An unknown error occurred when saving the file. Make sure the file is not open in another application and that the current user has write access to the requested location.
The Network Docent application detected that some files that are required for a proper operation are missing from the installation location.	-	Please close the Network Docent application and reinstall it. In case the problem continues to occur, a reboot might be required.
The Network Docent application is unable to set the promiscuous mode to the neighbor discovery driver.	-	The location of this computer in the network might not have been accurately detected and shown. A reboot might resolve this issue. Please note that not all network chipsets will support the promiscuous feature.
The Network Docent application detected that another instance of the application is actively scanning on this machine.	Only a single instance of the Network Docent application can scan at any given time.	In case no other instance is currently scanning, you can retry to start scanning in a few seconds. In case the problem continues to occur, a reboot might be required. This session will not start scanning at this time. See also *Troubleshooting an existing installation with a snapshot, page 52*.

9 Appendix

9.1 Glossary

SNMP

The Simple Network Management Protocol (SNMP) is widely used in network management for network monitoring. It can be used to collect and organize information about managed devices on IP networks. For instance the status of a disc drive, or the location of a printer. Many devices support SNMP, including switches, servers, printers, network-based audio devices etc. SNMP is part of the standard IP protocol. Network Docent Network Docent supports SNMP versions: SNMPv1, SNMPv2c and SNMPv3.

LLDP

The Link Layer Discovery Protocol (LLDP) is part of the IP protocol, and used by network devices for advertising their identity, capabilities, and adjacent devices (neighbors) on an Ethernet wired network. This information is discovered and stored in the LLDP MIB by the LLDP agent for retrieval by a SNMP based network management system, such as Network Docent. The LLDP agent is implemented as a default service for background operation on Windows. Windows 10 has an LLDP agent installed by default; this functionality is replaced by Network Docent's LLDP agent. LLDP performs functions similar to several proprietary protocols, such as Cisco Discovery Protocol, Foundry Discovery Protocol, Nortel Discovery Protocol and Link Layer Topology Discovery.

MIB

Management Information Base (MIB) is a text file that describes SNMP or LLDP network elements in readable English. These network elements are listed in the file as data objects. Every object referred to in an SNMP or LLDP message is listed and described in the MIB file, such as RFC1213-MIB2. To read the descriptions, Network Docent must have (read) access to this MIB file.

OID

An Object Identifier (OID) is an address used to identify devices and their statuses. OIDs are defined in the SNMP MIB file. Each time an SNMP device sends a message, it identifies each data object in the message with an OID or Object IDentifier. Network Docent uses the SNMP MIB as a dictionary for translating these OID numbers into human-readable text. The OCD's format is a long string of numbers. The first half of this string is defined by a standard referenced MIB used worldwide. The second half of the string is defined by the manufacturer of the device.

OCA

The Open Control Architecture (OCA) is a communications protocol architecture and is used for monitoring, controlling, and managing connections of networked audio and video devices. The official specification of OCA is the Audio Engineering Society (AES) open standard AES70 (or AES70-2015).

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com