LANCOM

Large Scale Monitor Manual

Large Scale Monitor Documentation

Stand: v1.30, 14.12.2015

LANCOM Systems

LANCOM Large Scale Monitor (LSM) contains the open-source components NAGIOS, CHECK_MK, NAGVIS and PNP4NAGIOS. The source code of the programs under GNU GPLv2. is on the DVD.

Contents

1 Introduction

The LANCOM Large Scale Monitor monitors the operation of LANCOM products. Designed especially for the WLAN access points, WLAN controllers, routers and switches from LANCOM Systems, it is ideal for monitoring mid-sized to large-scale installations.

It provides the following features:

- Scalable monitoring of 25 to 1000 devices
- Browser-based solution including smartphone support
- Adjustable triggers for alerts and notifications, incl. parent/child relationships
- Graphic display of floorplans with active status information
- User, role and rights management and the logging of changes
- Grouping of devices with configurable folder structures or topologies
- Monitoring and display of VPN connections
- Seamless roaming history for WLAN clients and LANCOM access points, even with complex client movements

Efficient operation of large-scale installations

The LANCOM Large Scale Monitor (LSM) is a professional tool for monitoring medium-sized to large-scale networks with 25 to 1,000 network components. Designed especially for LANCOM components including WLAN access points, controllers, switches and routers, this system based on open-source components additionally allows for the monitoring of third-party products such as servers and printers. Problems in the network are clearly displayed in tables or graphically on floor plans, and they trigger alert messages via e-mail if certain threshold values are not maintained.

Flexible options for installation

Commissioning the LANCOM LSM is made easy thanks to the variety of the packages available. LSM is installed from a bootable DVD, which also features a customized Linux distribution (CentOS) to get you started quickly. What's more, a variety of on-site installation services offers you support with your project installations.

Up to speed – always

The different user interfaces cater for a variety of different requirements for information. For instance, alerts and dashboards have been designed especially with smartphones in mind, so that system administrators and managers are constantly informed of the availability status.

Operators and support teams benefit from the clearly structured folder views and floor plan displays. The real-time status information they optionally display provides fast and intuitive access for fault diagnosis.

More than just a monitoring system

Another special feature is the seamless roaming history for WLAN stations. This facilitates the fast identification of errors from a central location, which is useful for example when troubleshooting signal-coverage problems experienced by moving WLAN clients. This type of problem is otherwise difficult to locate as data acquisition intervals are typically just 1 to 10 minutes. This greatly simplifies troubleshooting as the network history to the second from a WLAN client's perspective helps to provide a complete and seamless understanding.

The monitoring of VPN connections is greatly helped by the specialized and clearly structured display of all configured VPN connections.

2 Basics

Every network consists of individual, very different devices such as PCs, printers, access points, switches and routers.

General operation

The Large Scale Monitor now offers the possibility of checking the availability of devices by means of system-wide checks and, when threshold values are exceeded, alerts are generated in the form of notifications by e-mail.

However, output from the LANCOM Large Scale Monitor offers you much more than simple accessibility checks. Additional checks can be specifically configured for the devices. These provide additional information about device status, which can also be statistically processed and presented in various forms such as graphs or charts. The devices can be grouped to improve the clarity of the statistics. By way of example, a group can collect the devices according to the spatial structure of the organization.

Alarm system

Further to the monitoring and the representation of statistics, an integrated warning system sends messages by e-mail to registered addresses if threshold-value settings are exceeded.

Checks

With the help of the Large Scale Monitor, a range of checks can be sent to devices or groups of devices. These checks can be a simple query of device activity (ping) or they can supply a considerable amount of data about these devices via SNMP. This data can include the current throughput of the various LAN or WLAN interfaces, or even the actual device data stored in the device by the administrator.

A bulk discovery determines which meaningful checks can be directed to this device. You subsequently choose which of these checks should be used. A wide range of checks can be set for each type of device. It is also possible to configure a series of different checks at different time intervals (see section 5.16 "Time periods").

Views

The LANCOM Large Scale Monitor is a browser-based application and offers a wide range of views of the various devices on a network, their availability, and the data traffic.

Successful checks and their data sets can be represented in a number ways, as can the erroneous checks. Statistics can be compiled on the availability of individual devices and of groups of devices. It is also possible to display the different data sets for a single site or for any other organizational unit.

Representation of enterprise structures

Groups of devices can be created that represent both the spatial structure of the company and the organizational structures within it.

In this way, answers can be found to queries within an organization about the availability of a device or device failure. These answers can then be presented in a clearly structured, compressed or, if preferred, detailed form.

Tracking of WLAN devices

The LANCOM Large Scale Monitor is especially designed for the WLAN access points from LANCOM. They provide specific information about the WLAN stations logged on to them. Because this information is updated in short time intervals, the spatial movement of a station can be tracked by noting the various WLAN access points which the station logs on to. This allows the station's movement to be represented as a seamless chronological sequence.

User rights and roles

The level of detail of the display can be set by the role assigned to a user. Similarly, the right to configure new checks or thresholds or stop processes depend on which user is logged-on.

How does monitoring work?

Network components are monitored using checks of the different devices via Ping or, if supported by the devices, SNMP v2. This is a protocol defined as RFC (Internet standard) and which is based on IP (Internet Protocol). All LANCOM devices, along with most other network devices, support SNMP. The amount of information available from checks of the devices varies greatly, ranging from the simple availability (ping) to detailed information (SNMP) about the device's status (version and date of firmware, serial number, location, etc.) and the stations that are associated with LANCOM WLAN devices.

Display by browser

The LANCOM Large Scale Monitor is a web application that is installed on a server within the network. Multiple server instances can be collected into a cluster. The server presents all of the information so that all the user has to do is start a browser and connect to the Large Scale Monitor. Several users can be provided with different permissions. Where remote sites are monitored, the access connection needs to provide adequate data transfer. A secure connection (VPN) is recommended for this. The display has been tested for the MS Internet Explorer™, Mozilla Firefox™ and Chrome™, and there are displays especially for mobile devices such as the iPhone™ and Android™-based smartphones.

Easy installation

After installation, the software searches the network for available devices (network scan) or the devices to be monitored are imported via CSV file. The supported format of the CSV files matches that of the export files output by the LANCOM management tools (LCMS). The detected

devices are then presented to the administrator for final configuration, e.g. to be given meaningful names, their spatial or organizational classification, or for collection into groups.

Configuration and monitoring

In general we distinguish between user or device configuration and monitoring. Configuration involves the creation of devices, users, and structures. Only when these have been enabled are they monitored by the Large Scale Monitor. Monitoring is the active operation of the Large Scale Monitor. Actions, such as those for the snap-ins and views, are carried out on the enabled elements such as devices and checks.

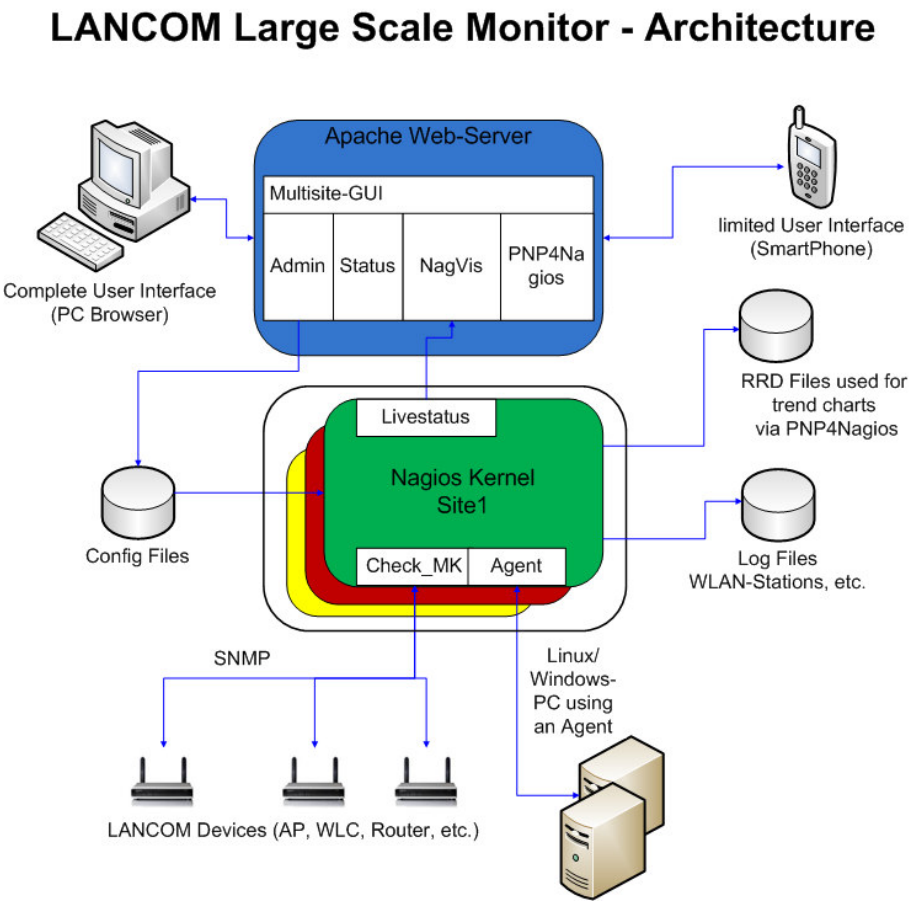
Licensing

Once the Large Scale Monitor has been set up, any type of configuration can be carried out. The Large Scale Monitor must be licensed if you wish to enable the devices or checks. The activation code is available from the LANCOM website.

2.1 LANCOM Large Scale Monitor architecture

The LANCOM Large Scale Monitor is based on a number of open source components including NAGIOS, CHECK_MK, MULTISITE, NAGVIS, PNP4NAGIOS and OMD. These modules have been supplemented by a browser-based LANCOM-specific user interface and by specialized monitoring functions developed for LANCOM devices (routers, WLAN access points, WLAN controllers and switches).

The overall framework for the Large Scale Monitor server is provided by OMD, the Open Monitoring Distribution, which handles the tasks of installation, management and updating. The operating system is CentOS 6.2, which forms the basis for the Large Scale Monitor server as a customized distribution. The following diagram provides an overview of a Large Scale Monitor server's main components:



The core and the checks

At the heart of the LANCOM Large Scale Monitor is the Nagios core, which is known worldwide and which operates in millions of installations. The task of the core is to actively trigger checks, to manage the current status and parameters of all monitored devices/hosts, and to detect status changes (for example, if a device changes from OK to CRITICAL).

The software CHECK_MK is responsible for the efficient processing of status checks. The checks are handled on the one hand by means of an agent, which is available for all major operating systems, and via SNMP, which is in widespread use for monitoring network devices, appliances, temperature sensors, and similar devices. LANCOM devices are also queried via SNMP. Only the basic network checks such as PING, DNS queries or checks via HTTP continue to run with standard Nagios plug-ins. The advantages of Check_MK compared to standard checks are:

- High performance

  A monitoring server can query ten times as many devices with Check_MK. The checks can also be considerably more detailed.

- Automatic bulk discovery

  Check_MK independently detects the parameters to be monitored, including for devices that are monitored by SNMP. Even in complex and changing environments, this ensures that the configuration of the monitoring remains simple and straightforward.

Interface components (GUI)

The LIVESTATUS interface provides efficient access to the status data in the core and acts as a data interface for the visualization components. LIVESTATUS replaces Nagios' very slow interface without the additional effort of using an SQL database.

The component CONFIG is a comprehensive configuration interface for the LANCOM Large Scale Monitor server. A web-based user interface is used for the efficient configuration of devices and checks, triggers, threshold values, users, groups, and roles, and all the other important settings made.

NagVis is the most popular visualization solution for Nagios. It represents current status data on customizable maps.

NPNP4Nagios is responsible for the recording of measurement data over a longer period (e.g. the memory usage of a computer or the load on a switch port). This facilitates the display of time series and graphics. The highly efficient RRDTool is used as the storage backend.

3 The main page

This section provides a general overview of the main page of the Large Scale Monitor. The Large Scale Monitor is invoked by entering the Large Scale Monitor's URL into a web browser. After the login procedure, the dashboard "WLAN" is displayed as the main page. This section explains the structure and function of the various sections of this dashboard.

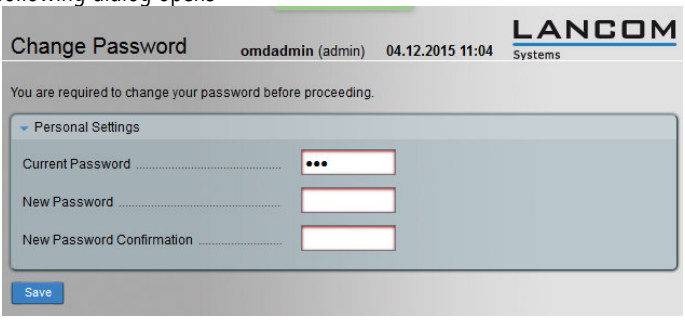
Optionally, another dashboard "VPN" can be selected as the default. Please refer to section 5.8 "Global settings" for more information.

How to connect to the Large Scale Monitor

1. In your web browser, enter the address of the Large Scale Monitor server (e.g. "lsm-server"). The browser connects to the server and first shows the login screen.

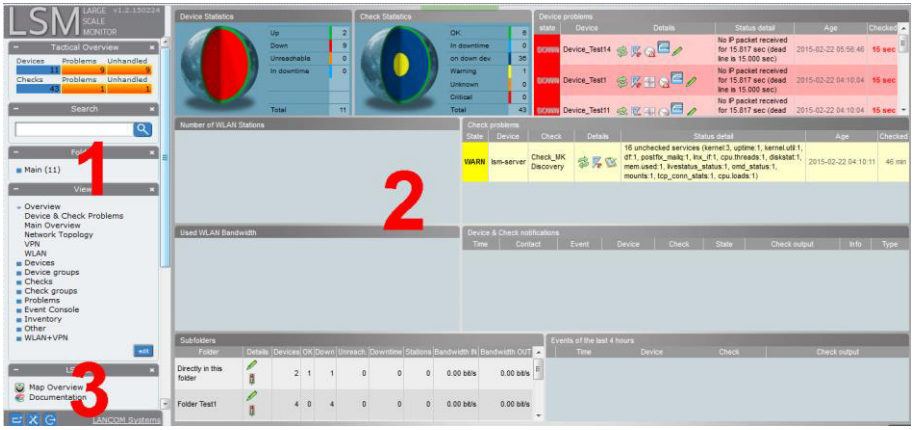
2. The first time you connect, enter the default user name "omdadmin" and the password "omd". Please note that entering a user name and password is case sensitive!

   The following dialog opens



3. First enter the old password ("omd") and then set a new password. Observe the password policy when setting the password, and select at least six characters from three of these four groups: A-Z, a-z, 0-9, and special characters. Please note that entering a user name and password is case sensitive!

   The first page of the Large Scale Monitor opens up.



The LANCOM Large Scale Monitor user interface is divided into three parts, the side bar (1), the main section (2) and the menu bar (3).

➢ In order for the Large Scale Monitor to be displayed to the optimum, a full screen in the web browser with a screen resolution of 1600x1024 or larger is recommended.) If this is not available, you can reduce (Ctrl-) or increase (Ctrl+) the view in the browser.

3.1 Sidebar

The side bar is displayed on the left (1). Snap-ins that have been installed are displayed here. Detailed explanations about this and other functions are available in section 7 "Snap-ins".

Snap-in	Description
Tactical overview	Shows the overall number of devices being monitored, the total number of individual checks, the number of the problems it encountered, and the number of unhandled cases. Please refer to section 7.1.2 "Tactical overview" for further information.
Search	Helps to search for devices. Entering the first letter displays a list of choices. Please refer to section 7.1.3 "Search" for further information.
Folders	Shows an overview of the folders that have been created. Select a topic and a corresponding view in the drop down list and then click on one of the folders; this selected view is then displayed in the main window (2). This always relates to the sub-folder selected in the tree structure. Please refer to section 7.1.4 "Folders" for further information.
Views	A list of the different views. Here, you can determine which view you want to see on the right-hand side. The view you select here always relates to the entire network. Please refer to section 7.1.5 "Views" for further information.
LSM Links	Provides a map overview of the various folders for the entire network. Please refer to section 7.1.6 "LSM Links" for further information. Here you will also find a link to the documentation.
CONFIG **- Configuration**	Opens the Large Scale Monitor's configuration program. Please refer to section 7.1.7 "CONFIG – Configuration" for further information.

Hide and show side bar

You can hide the side bar by clicking in the snap-in field on the left-hand side of the LSM window. Display the side bar again by clicking on the left frame.

You will find a menu bar at the bottom of the side bar (3):

This menu bar offers you quick access to the following functions:

	Add another snap-in to the side bar. Please refer to section 7.2 "Edit snap-ins" for further information.
	Change the profile of the currently logged-on user, i.e. the language and the password. Please refer to section "Personal settings" for further information.
	Log off the current user. The login input mask is then displayed. Please refer to section "How to connect to the Large Scale Monitor" for further information.

	This icon only appears if the user has been sent a message. Click on the icon to read the message. Please refer to section 5.12.3 " Spontaneous notificationSpontaneous notification" for more information on instant messaging.
	More information about the current version of the Large Scale Monitor and its installed components.

3.2 Main section

Here you find either a dashboard or a view, e.g. a table. A dashboard combines various informational elements such as tables, time series, pie charts, and so on. They usually refer to the overall network. The dashboard view can be limited to a subtree simply by selecting it.

The arrangement and the selection of information elements on the dashboard can be changed. There are a number of pre-configured dashboards (see "Pre-configured dashboards"). Section 6.9 "Creating and modifying dashboards" shows you how to change these pre-settings.

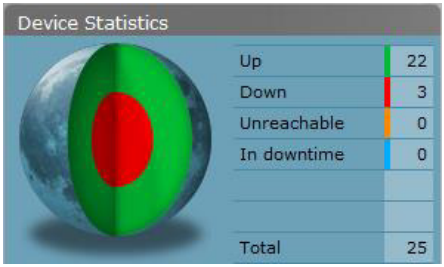
► If there is no information for the selected folder, the field remains empty.

The information is refreshed every 30 seconds.

You can always access the dashboard for the entire network by clicking on the product name at the top of the side bar:

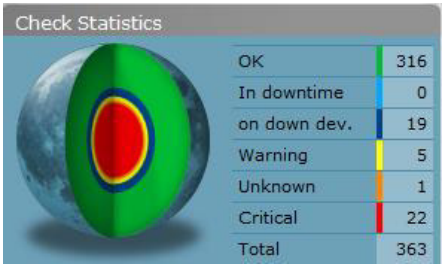
The main overview displayed by default after installation consists of the following information elements:

Device statistics



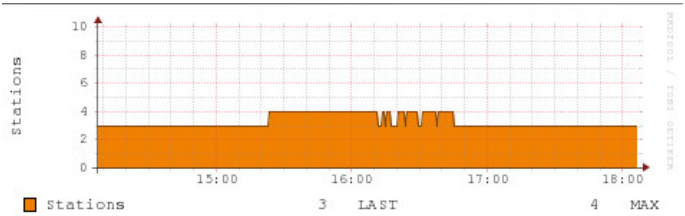
This displays the current status of the devices. Please refer to section 6.1.3 ""Devices" views" for further information.

Check statistics



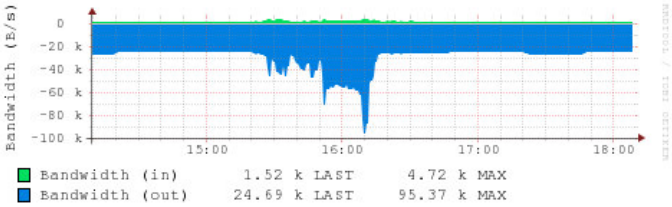
This displays the success rates of the current checks. Please refer to section 6.1.6 ""Check groups" views" for further information.

Number of WLAN stations



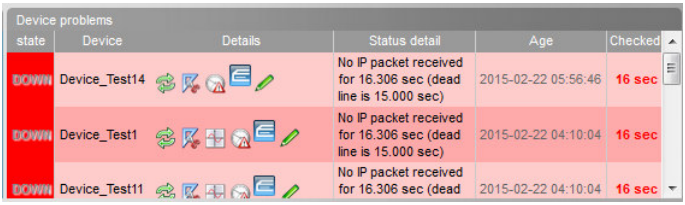
Shows the chronological sequence of the associated WLAN stations. Please refer to section 6.1.6 ""Problems" views" for further information.

Used WLAN bandwidth



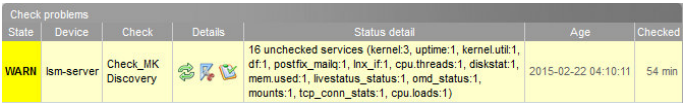
Shows the time series of the WLAN bandwidth in use.

Device problems



Displays the list of devices which are having problems. The list is initially sorted chronologically. Please refer to section 6.1.3 ""Devices" views" for further information.

Check problems



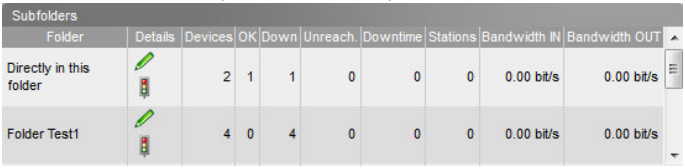
Displays the devices for which checks are currently causing a problem. The list is sorted according to the seriousness of the problems. Please refer to section 6.1.3 ""Devices" views" for further information.

Notifications over the last 4 hours

Provides an overview of the notifications sent by the Large Scale Monitor ordered by recency.

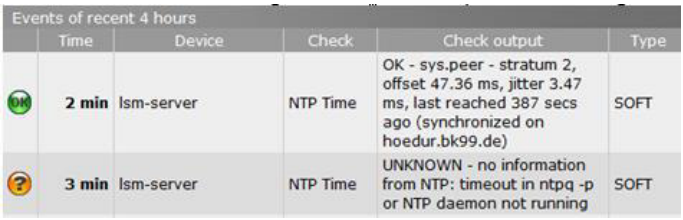
Subfolders

Displays the subfolders for the levels currently displayed as well as some of their properties such as the number of devices contained, their downtimes, etc.



Events over the last 4 hours

Provides an overview of the most recent events.



Events of recent 4 hours

	Time	Device	Check	Check output	Type
OK	2 min	lsm-server	NTP Time	OK - sys.peer - stratum 2, offset 47.36 ms, jitter 3.47 ms, last reached 387 secs ago (synchronized on hoedur.bk99.de)	SOFT
?	3 min	lsm-server	NTP Time	UNKNOWN - no information from NTP: timeout in ntpq -p or NTP daemon not running	SOFT

Main overview header

The header of the main overview provides information about the currently logged-on user, the user's role which sets the user rights, the current time of the Large Scale Monitor server, and a link to the LANCOM home page in the form of the company logo.

4 Installing the Large Scale Monitor

The Large Scale Monitor is installed from a DVD. All software required is delivered on this DVD and installed on a computer provided by the customer (see Chapter 4.2 “Running the installation”).

4.1 Hardware requirements

The following requirements apply to the computer on which the LANCOM Large Scale Monitor is installed as a server.

For operation	
Processor	2.8 GHz Quad-Core CPU as a minimum
RAM	8GB RAM (16GB preferred)
Hard drive	100GB
Network card	

Additional alternatives for the installation	
DVD drive	Installation from DVD
USB stick	USB flash drive (minimum 2 GB)

An additional requirement is access to the network and possibly a DHCP server on the network. Further computers on the network can be used for remote administration.

4.2 Running the installation

Two options are available for installing the Large Scale Monitor:

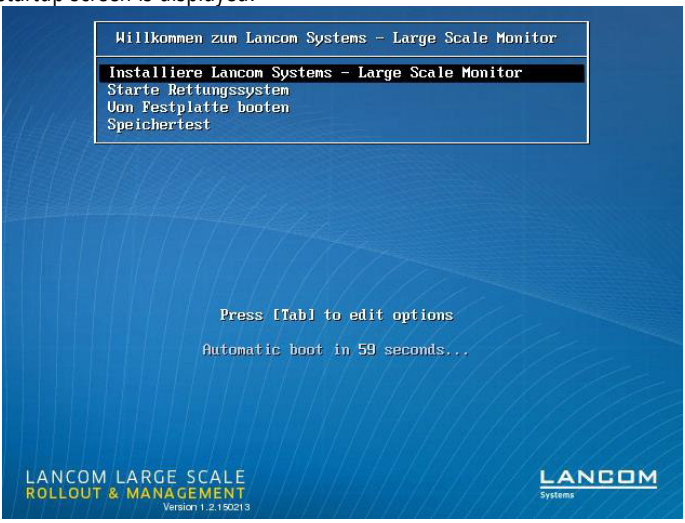
- Installation directly from the DVD. For detailed instructions see the section "How to install the LANCOM Large Scale Monitor from DVD".
- Installation from a USB stick (minimum size of 2 GB). For detailed instructions see the sections "How to prepare the bootable USB stick" and "How to install the LANCOM Large Scale Monitor from a USB stick".

For both of these installations, the hard drive is reformatted and Linux (CentOS Version 6.7) is installed as the operating system. All data on the hard drive are erased in the process.

How to install the LANCOM Large Scale Monitor from DVD

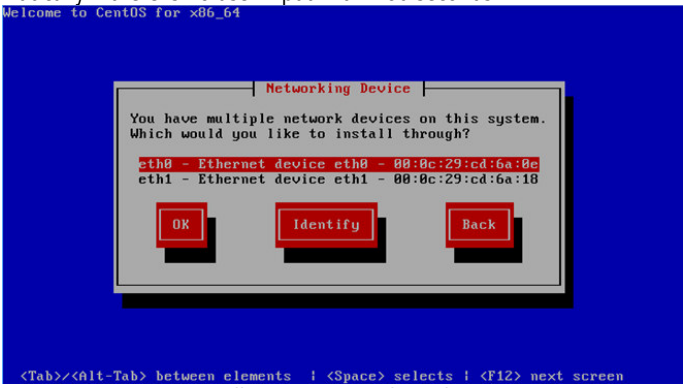
1. Insert the DVD into the DVD drive of the computer and boot the PC.

   The startup screen is displayed.



Installation - Start

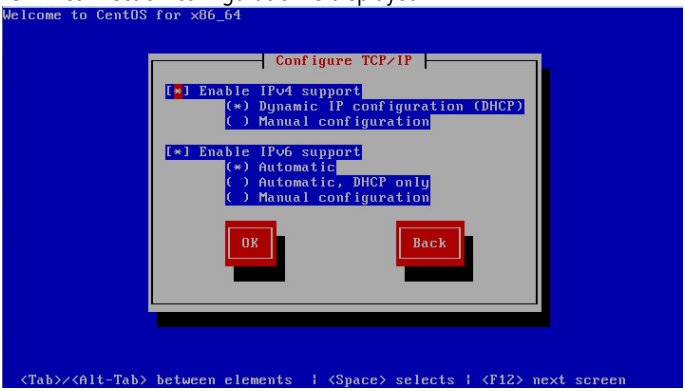
2. Select the "Install LANCOM Systems - Large Scale Monitor". This option is selected automatically if there is no user input within 60 seconds.



Installation – Networking device

3. If the server has multiple Ethernet interfaces, select the one to be used for communication by the LSM.

The installation of the Linux system starts.
The TCP/IP connection configuration is displayed.



Installation – TCP/IP cofiguration

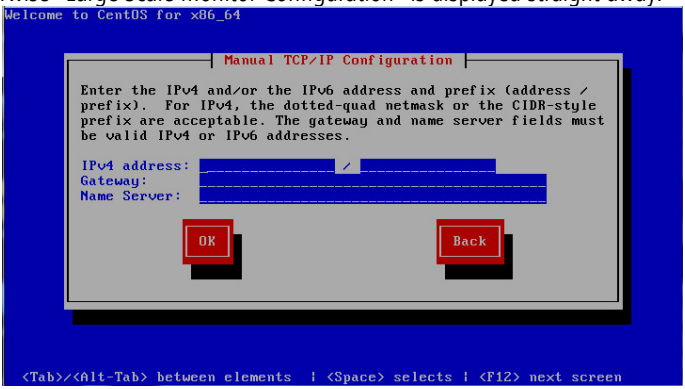
4. The network configuration of the server is entered here.

   Use the TAB key (or ALT-TAB) to move through the entries. Select an option with the space bar. If there is a DHCP server in the network, you can select:

   - For IPv4 support: "Dynamic IP configuration (DHCP)"
   - For IPv6 support: "Automatic"

5. Confirm your selection with "OK".

   Wait for the network adapter to be configured.
   If you have selected a manual entry, "Manual TCP/IP Configuration" is displayed; otherwise "Large Scale Monitor Configuration" is displayed straight away.

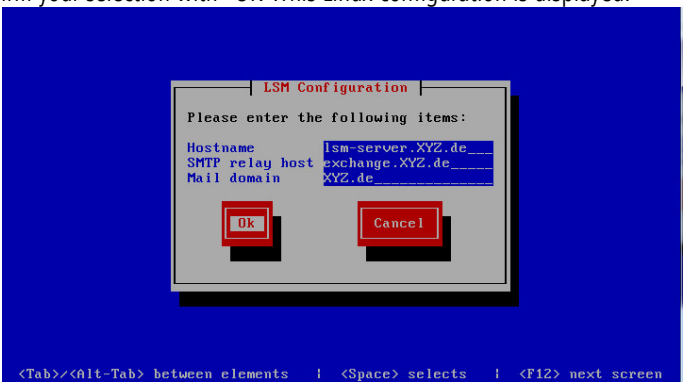


Installation – Manual TCP/IP configuration

6. Manually enter the required data here:

- IP address and network mask of the server for IPv4
- IP address and network mask of the server for IPv6 (optional)
- IP address of the gateway
- IP address of the name server

Confirm your selection with "OK".This Linux configuration is displayed:



Installation – LSM configuration

7. Enter here the parameters for the server:

   - Host name

     Name of the servers in the format <Name>.<Domain> – e.g. lsm-server.XYZ.com

   - SMTP relay host

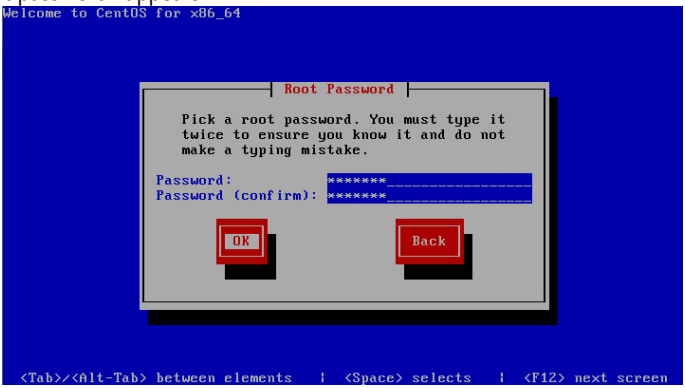
     Name of the SMTP server, e.g. exchange.XYZ.com

   - Mail domain

     Necessary for sending e-mails from the Large Scale Monitor, e.g. XYZ.com

8. Use TAB to change to "OK" and confirm with the RETURN key.

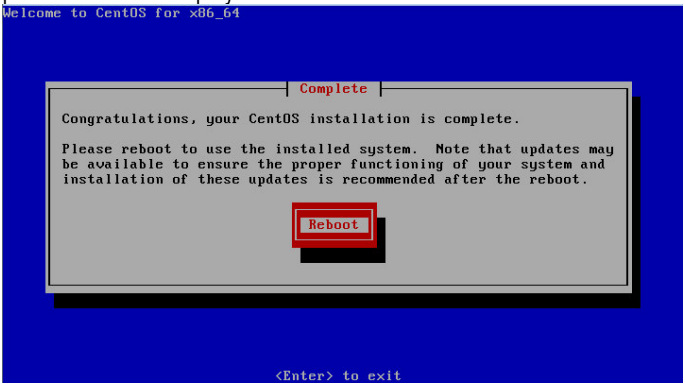
"Root password" appears.



Installation – Root password

9. Enter here the password for the Root Administrator for this Linux installation and confirm by entering it again.

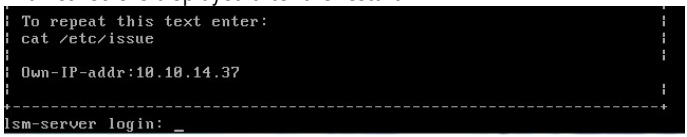
   Observe the password policy when setting the password, and select at least six characters from three of these four groups: A-Z, a-z, 0-9, and special characters.
   The Linux installation is run afterwards. This may take a few minutes.
   A request to restart is displayed.



Installation – Restart

10. Remove the DVD from the drive.
11. Use TAB to change to "Reboot" and confirm with the RETURN key.

The Linux console is displayed after the restart.



Installation – Linux console

The Large Scale Monitor is now ready for use. No more actions are required on this computer. Switch the monitor off or remove it. The rest of the configuration is performed from another computer over the web interface.

12. Switch to the web browser of another computer in the same network.
13. Enter the following URL in the browser:

    `https://<Name or IP address of the LSM server>`

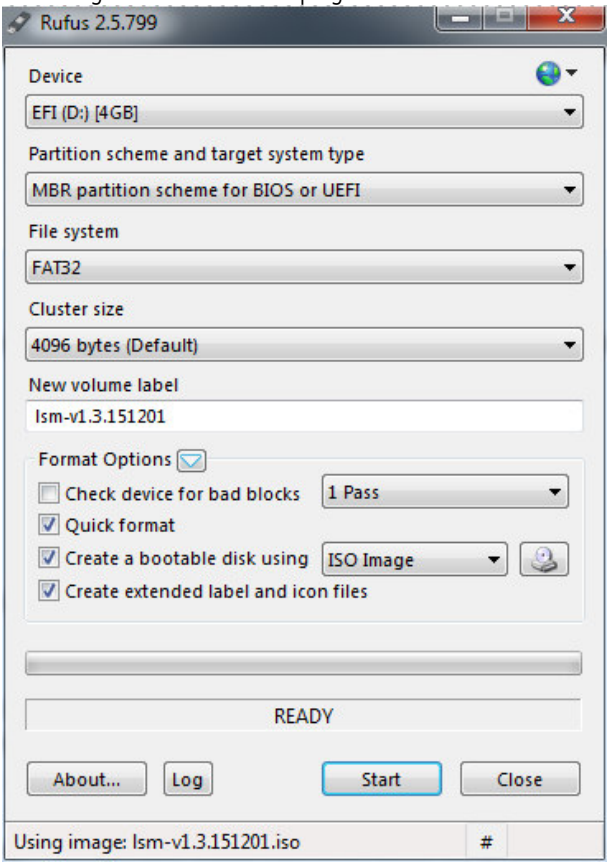
Please refer to section 5 "Configuration" for further configuration steps.

► After reinstalling, the Check_MK Micro Core is applied (as of version 1.20). For details on how to change the core, see section 4.5 "Changing the monitoring core".

How to prepare the bootable USB stick

1. Requirement:
   - The USB stick needs at least 2 GB of memory.
   - The Large Scale Monitor is available as an .iso image.
2. To install the Large Scale Monitor from a USB stick you need a bootable USB flash drive. Choose a utility to make the USB stick bootable. The utility "Rufus" that is explained here is available from http://rufus.akeo.ie.
3. Download the "Rufus" program to a Windows PC.
4. Make sure that the .iso image of the LSM is available on this PC.
5. Start the "Rufus" utility.

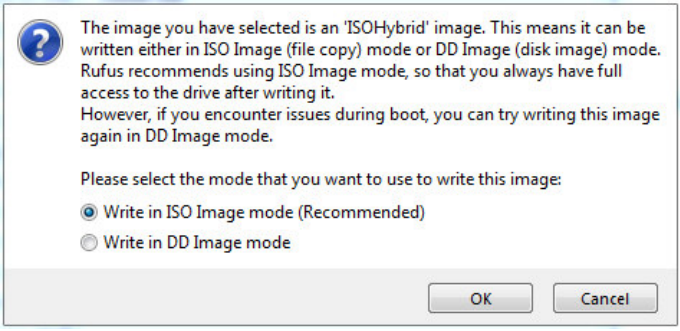
   This opens a dialog box for the "Rufus" program.



Installation – "Rufus" utility for configuring a bootable USB stick

6. Set the "Device" to the USB stick and set the "Partition scheme" to "MBR partition scheme for BIOS or UEFI". Select the checkbox "Create a bootable disk using", select the option "ISO Image" and enter the path to the .iso image file for the LSM.
7. Start Rufus.

   A dialog opens



8. Choose the recommended option “Write in ISO Image mode” and confirm with OK.

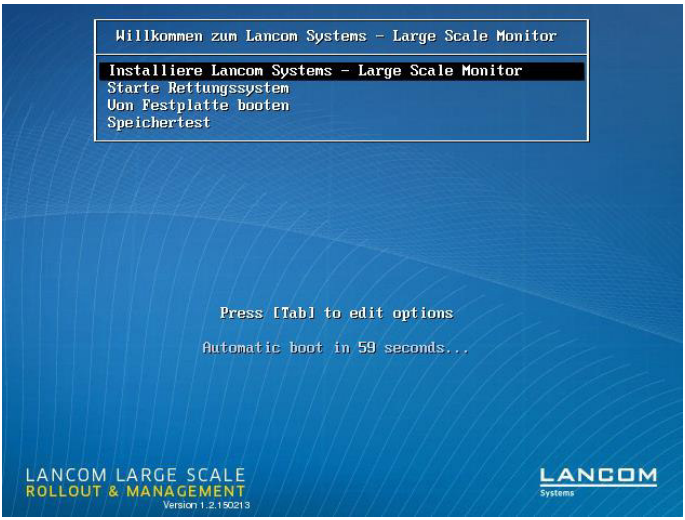
   This creates a bootable USB stick, which will immediately start installing the Large Scale Monitor on a freshly booted PC.

How to install the LANCOM Large Scale Monitor from a USB stick

Requirement: You need a bootable USB stick (see section "How to prepare the bootable USB stick")

1. The server must be able to boot from a USB stick (BIOS settings).
2. Plug the LSM USB stick into the server and start it.

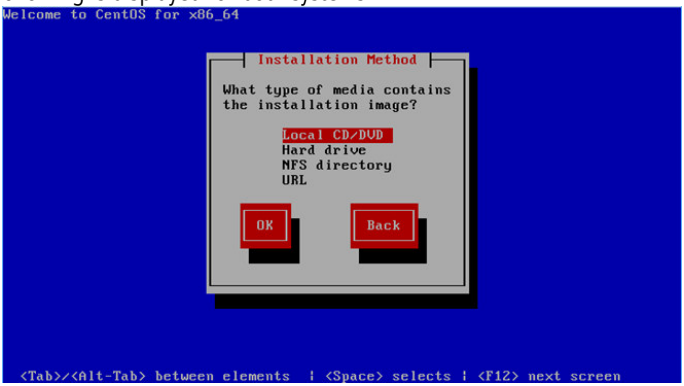
The installation starts in accordance with the BIOS or UEFI settings in the server BIOS. A server operating with the standard BIOS will display the start screen, whereas UEFI skips this.



Installation - Start

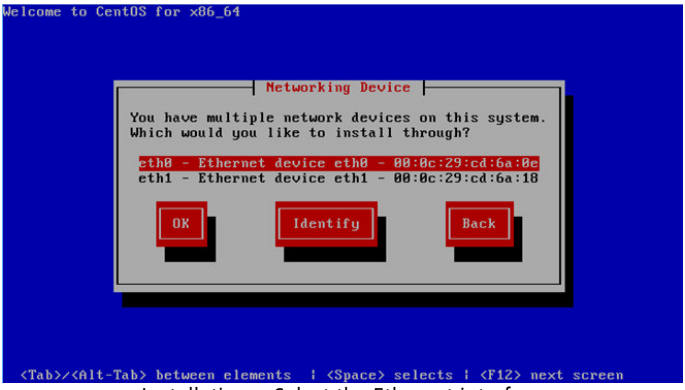
3. Select the item "Install LANCOM Systems – Large Scale Monitor". This option is selected automatically if there is no user input within 60 seconds.

   The following is displayed for both systems



Installation – Method

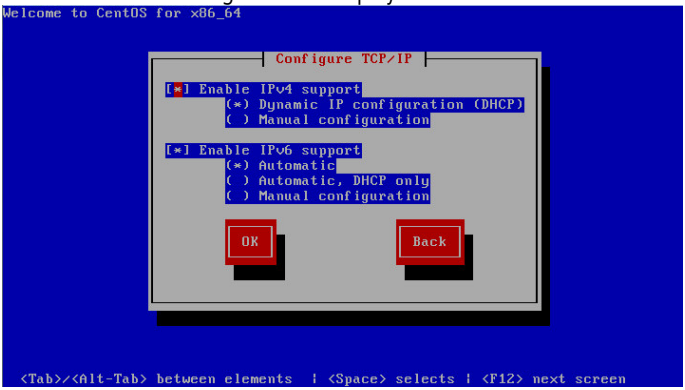
4. Select "Hard drive" and confirm with "OK". The USB stick is then mounted as a hard drive.



Installation – Select the Ethernet interface

5. If the server has multiple Ethernet interfaces, select the one to be used for communication by the LSM.

   The installation of the Linux system starts.
   The TCP/IP connection configuration is displayed.



Installation – TCP/IP configuration

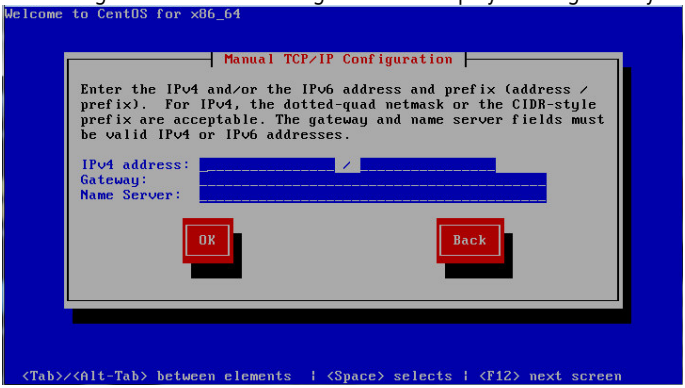
6. The network configuration of the server is entered here.

   Use the TAB key (or ALT-TAB) to move through the entries. Select an option with the space bar. If there is a DHCP server in the network, you can select:

   - For IPv4 support: "Dynamic IP configuration (DHCP)"
   - For IPv6 support: "Automatic"

7. Confirm your selection with "OK".

Wait for the network adapter to be configured.
If you have selected a manual entry, "Manual TCP/IP Configuration" is displayed; otherwise "Large Scale Monitor Configuration" is displayed straight away.

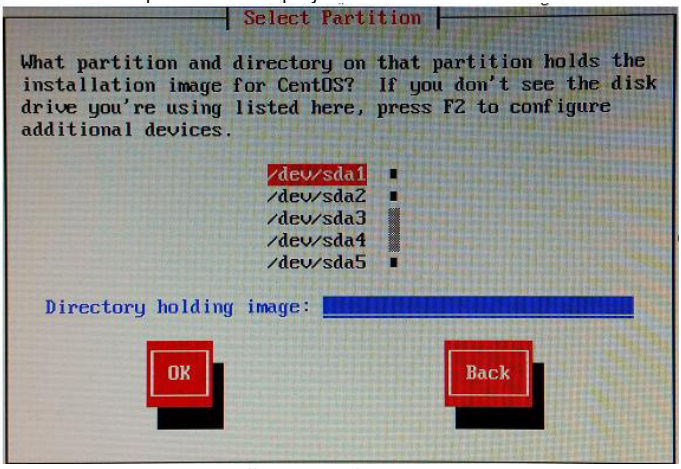


Installation – Manual TCP/IP configuration

8. Manually enter the required data here:

- IP address and network mask of the server for IPv4
- IP address and network mask of the server for IPv6 (optional)
- IP address of the gateway
- IP address of the name server

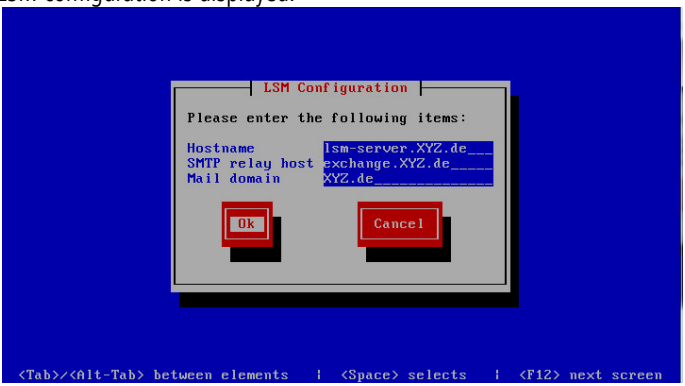
Confirm your selection with "OK".
The selection of the partition is displayed.



Installation – Select Partition

9. Choose the partition which holds the installation image for CentOS. You don't have to enter a path to the directory. Confirm the selection with OK.

   The LSM configuration is displayed:



Installation – LSM configuration

10. Enter here the parameters for the server:

    - Host name

      Name of the servers in the format

      - <Name>.<Domain> – e.g. lsm-server.XYZ.com

    - SMTP relay host

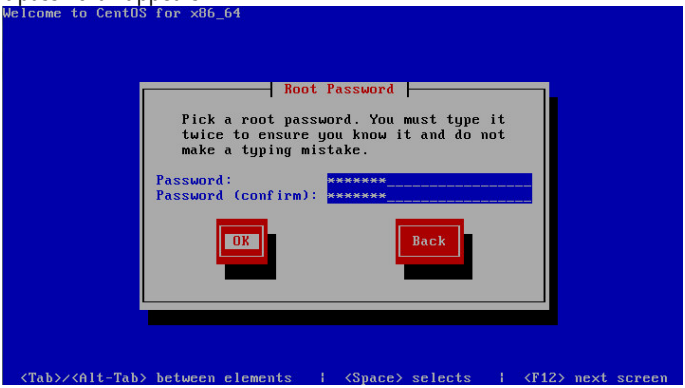
      Name of the SMTP server, e.g. exchange.XYZ.com

    - Mail domain

      Necessary for sending e-mails from the Large Scale Monitor, e.g. XYZ.com

11. Use TAB to change to "OK" and confirm with the RETURN key.

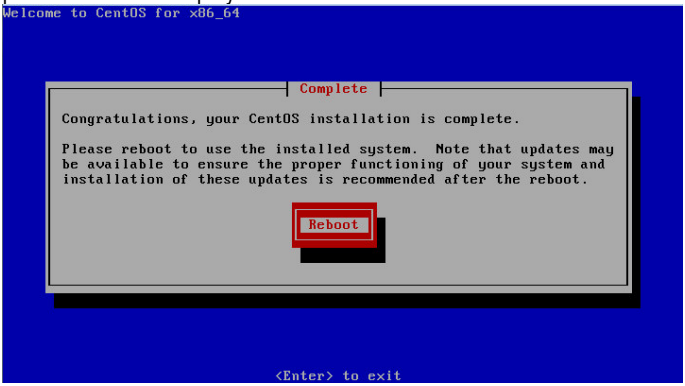
"Root password" appears.



Installation – Root password

12. Enter here the password for the Root Administrator for this Linux installation and confirm by entering it again. ,,

    Observe the security requirements for the password and select characters from three of these four groups: A-Z, a-z, 0-9, and special characters.
    The Linux installation is run afterwards. This may take a few minutes.
    A request to reboot is displayed.



Installation – Reboot

13. Remove the USB stick.
14. Use TAB to change to "Reboot" and confirm with the RETURN key.

The Linux console is displayed after the restart.

Installation – Linux console

The Large Scale Monitor is now ready for use. No more actions are required on this computer. Switch the monitor off or remove it. The rest of the configuration is performed from another computer over the web interface.

15. Switch to the web browser of another computer in the same network.
16. Enter the following URL in the browser:

    `https://<Name or IP address of the LSM server>`

    Please refer to section 5 "Configuration" for further configuration steps.

► After reinstalling, the Check_MK Micro Core is applied. For details on how to change the core, see section 4.5 "Changing the monitoring core".

4.3 Changing the mail configuration

The following commands are available to change the mail configuration:

- Display the mail relay: postconf -v relayhost
- Display the mail domain: postconf -v mydomain
- Set the mail relay: postconf -e relayhost=<10.10.10.10>
- Set the mail domain: postconf -e mydomain=<maildomain.de>

4.4 Update

If a Large Scale Monitor is already installed, the server can be updated to version v1.30.

Requirements

You already have an LSM server installed and running with an older version. You need the current version of the LSM on a DVD or as an ISO image.

If the server does not have a console or a DVD drive and can only be accessed via a network, then you need additional utilities to access the LSM from a Windows environment.

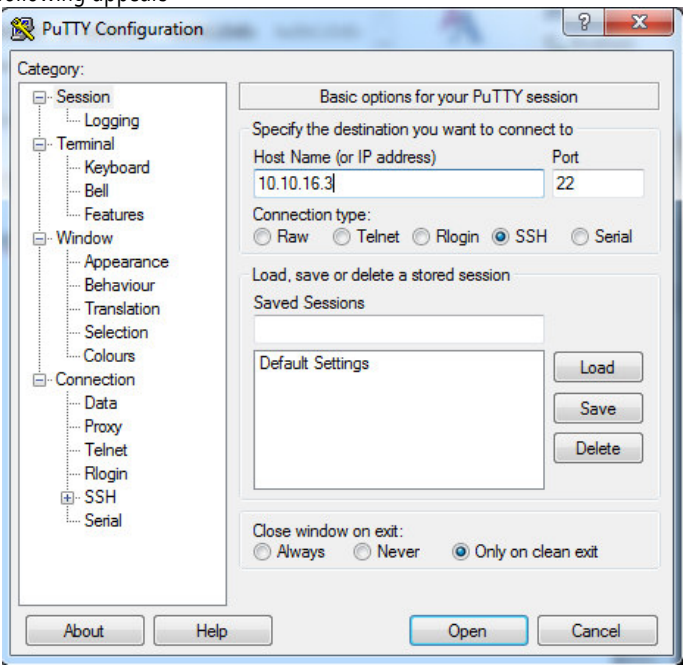
- PuTTY for the administration console during the update
- WinSCP to copy the files from the DVD or the ISO image to the Linux server
- WinRAR for direct access to the files in an ISO image

Download these free programs from the internet.

How to update the LANCOM Large Scale Monitor

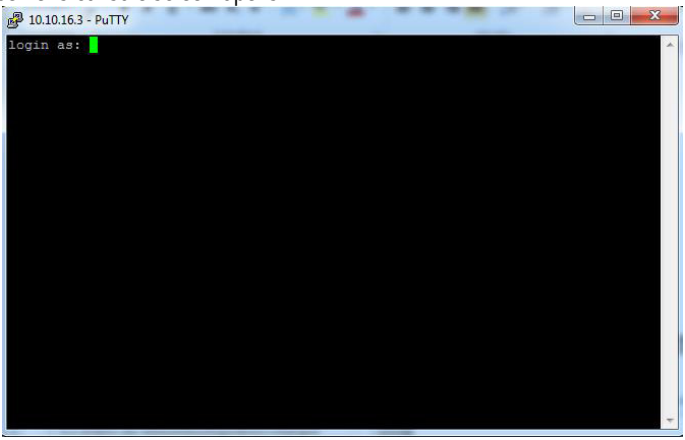
1. Call up the PuTTY utility.

   The following appears



2. Enter the IP address of the LSM server and leave the remaining default settings.
3. Click on "Open" and confirm the trusted connection to the server.

The server's console screen opens.



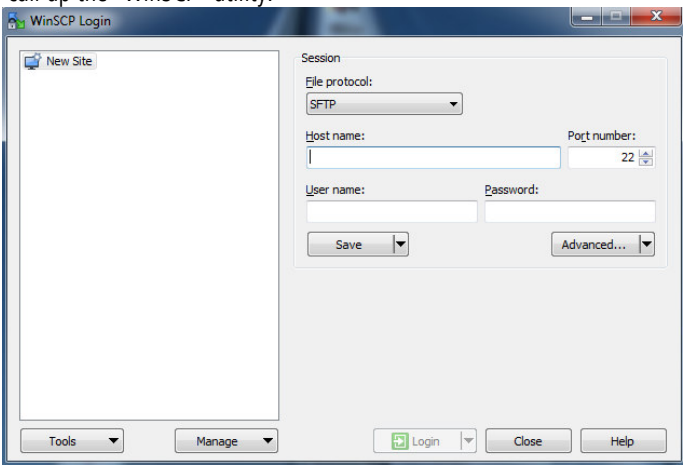
4. Log in here as the root administrator.

   To do this, enter

   ```
   Login as:root
   ```

   and confirm your entry with RETURN. For the password, use the one you selected during the installation (see "Running the installation"). Default is "lsmlsm". Pay attention to upper/lower case.

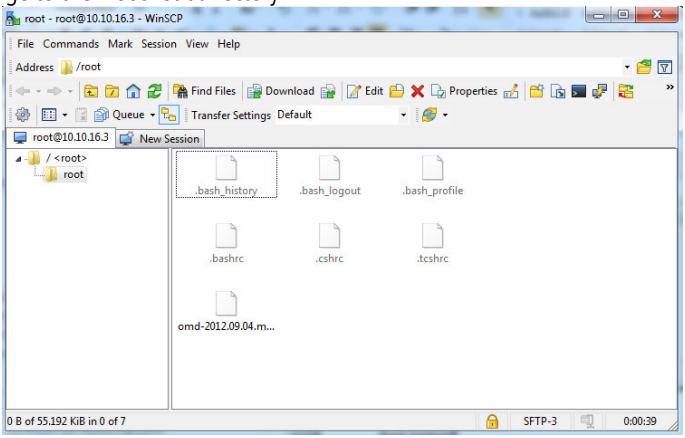
5. Now call up the "WinSCP" utility.



6. Enter here the LSM server's IP address, the "root" user name, and the root administrator's password (default: "lsmlsm").
7. Click on "Login" and confirm the trusted connection to the server.

The file system of the LSM server is displayed.

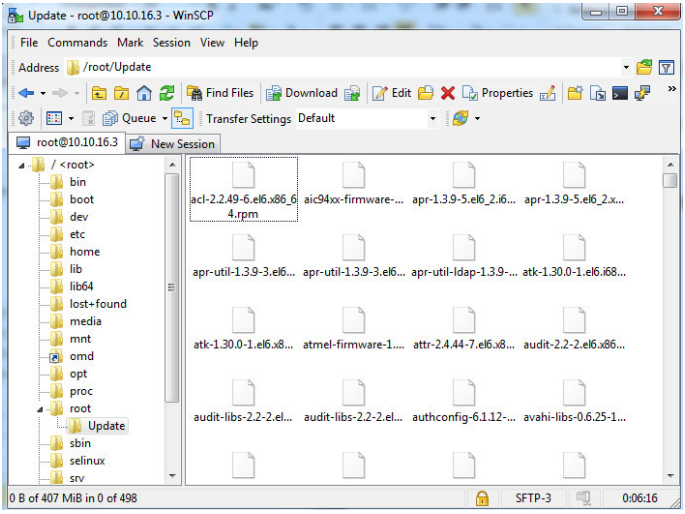
8. Change to the "root" subdirectory



9. In this directory, create a new sub-directory "Update" by right-clicking on the right-hand field of the display and selecting "New | Directory" in the menu.
10. Open the "LSM | update" directory, e.g. with the Explorer on the DVD or with WinRAR in the ISO image.

    You will see a number of RPM files

11. Copy these RPM files by drag&drop into the newly created "Update" directory and onto the LSM server.



12. Then close WinSCP and switch back to the console display in PuTTY.

13. Change to the update directory with

```
[root@<computer name> ~]#cd Update
```

Again, pay attention to upper/lower case.

14. Display the available LSM version with

```
[root@<computer name> Update]#omd versions
```

The current version appears, e.g.

```
lsm-v1.2.150313 (default)
```

15. Enter at the command line

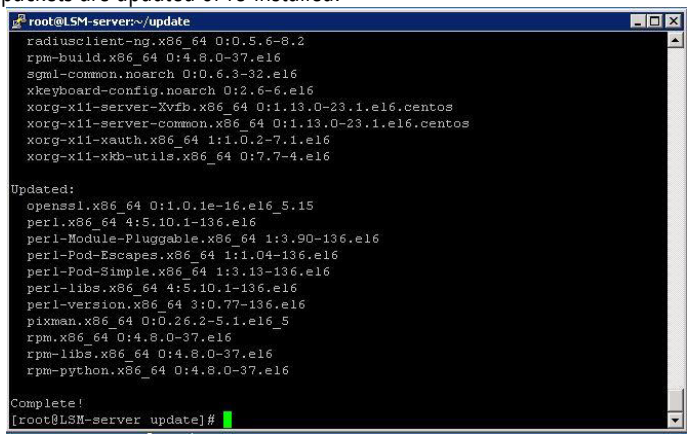
```
[root@<computer name> Update]#yum install --
disablerepo=* *
```

End your entry with RETURN.

16. Confirm the installation with "y".

```
[root@<computer name> Update]# y
```

The packets are updated or re-installed.



This command line is displayed again

```
[root@<computer name> Update]#
```

17. Display the available LSM version again with

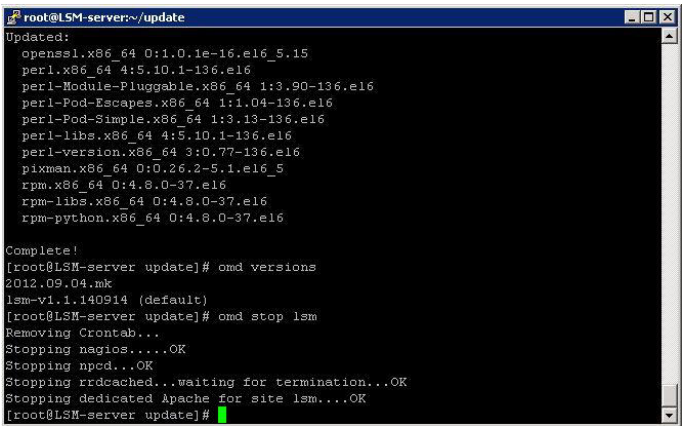
```
[root@<computer name> Update]#omd versions
```

Both versions are now displayed, e.g.

```
lsm-v1.2.150313
lsm-v1.3.151031 (default)
```

18. Halt the LSM with the command:

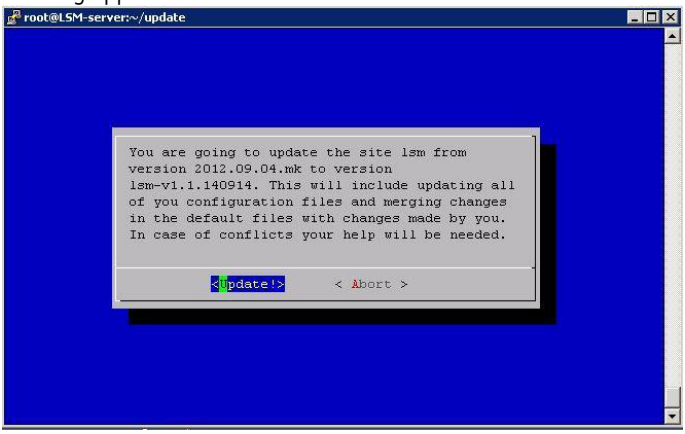
```
[root@<computer name> Update]# omd stop lsm
```



19. Start updating the version with

```
[root@<computer name> Update]# omd update lsm
```

The following appears



20. After confirming the "Update!" selection with RETURN, different entries are now displayed.

    You may see some conflicts announced in the following ways:

    - Conflict "version changes"

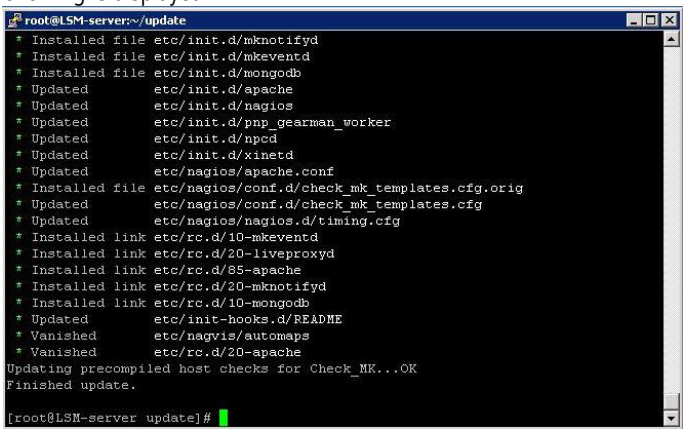
I've tried to merge the changes from version 2012.09.04.mk to lsm-v1.01.130612
into etc/check_mk/conf.d/wato/rules.mk. Unfortunately there are conflicts with your changes. You have the following options:
diff Show differences between the new default and your version
you Show your changes compared with the old default version
new Show what has changed from 2012.09.04.mk to 2013.02.07.mk
edit Edit half-merged file (watch out for >>>>> and <<<<<)
try again Edit your original file and try again
keep Keep half-merged version of the file
restore Restore your original version of the file
install Install the new default version
shell Open a shell for looking around
abort Stop here and abort update!
d/y/n/e/t/k/r/i/s/a ==>

In this case, enter "i" and close with RETURN.

- Conflict "Wrong permission"

Wrong permission of etc/check_mk/conf.d/wato/contacts.mk
The proposed permissions of etc/check_mk/conf.d/wato/contacts.mk are 0644,
But currently are 0660. May I use the new default permissions or keep yours?
keep Keep permissions at 0660
default Set permission to 0644
shell Open a shell for looking around
abort Stop here and abort update!
k/d/s/a ==>

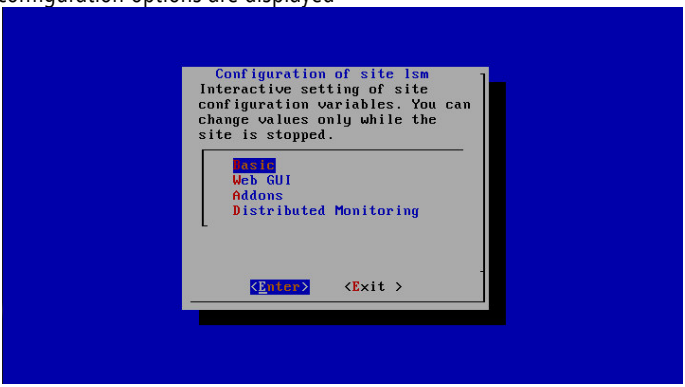
In this case, enter "d" and conclude with RETURN.
The following is displayed:



21. Check that all the services required by the LANCOM Large Scale Monitor are enabled.
To do this, enter

```
[root@<computer name> Update]# omd config lsm
```

The configuration options are displayed



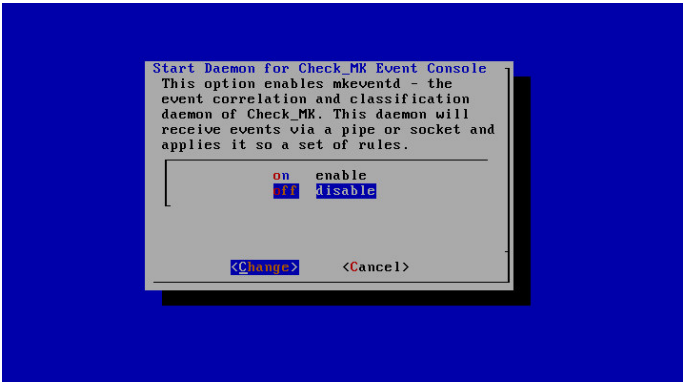
22. Choose "Addons" and confirm your selection with RETURN.

A summary of the services and their status is displayed

The services MKEVENTD, MKEVENTD_SYSLOG and MKNOTIFYD must be enabled ("on").

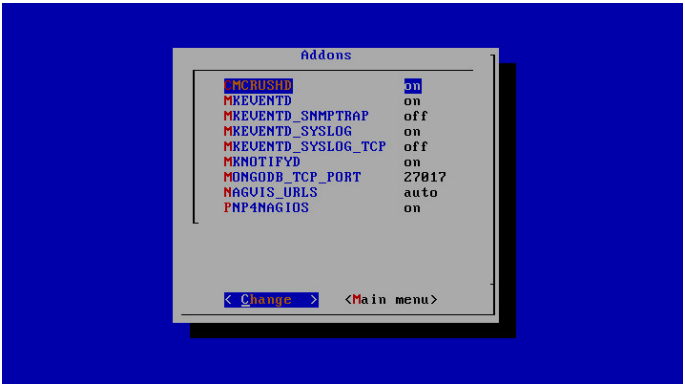
23. If a service is not enabled ("off"), select it with the arrow keys and confirm the selection with RETURN (here: MKEVENTD).

The start page for the corresponding service is displayed (here: MKEVENTD).



24. Use the arrow keys to select "on" and confirm with RETURN.

The summary of services is displayed again, this time enabled (here MKEVENT)



25. Navigate with the arrow keys to the "Main menu" and confirm with RETURN.

    This configuration overview is displayed again

26. Press "Exit" and RETURN.

    This command prompt is displayed again

    ```
    [root@<computer name> Update]#
    ```

27. Then restart the LANCOM Large Scale Monitor with

    ```
    [root@<computer name> Update]# omd start lsm
    ```

28. This input line is displayed again

    ```
    [root@<computer name> Update]#
    ```

    This concludes the update and the LSM can be accessed via the web browser once again.

► The core is retained during the upgrade. For details on how to change the core, see section 4.5 "Changing the monitoring core".

4.5 Changing the monitoring core

As of 1.20, a new installation installs the Check_MK Micro Core instead of the Nagios core. It requires less processor resources, but more memory. For this reason a memory of 8 GB is required (and better 16 GB).

Updating older installations may result in a switch to the Check_MK Micro Core (cmc).

How to change the monitoring core

1. Log into the Linux console on the Large Scale Monitor server as user "root" with the password assigned in the administration.

   This Linux prompt is displayed:

   ```
   [root@<computer name> ~]#
   ```

2. Enter:

   ```
   [root@<computer name> ~]# omd stop lsm
   ```

   The command line is displayed once the server has stopped:

   ```
   [root@lsm-server ~]#
   [root@lsm-server ~]# omd stop lsm
   Removing Crontab...OK
   Stopping dedicated Apache for site lsm.................OK
   Stopping Check_MK Micro Core...killing 1303............OK
   Stopping CMC Rushing Ahead Daemon...killing 1291....OK
   Stopping rrdcached...waiting for termination...OK
   Stopping mknotifyd...killing 1275...
   Stopping Livestatus Proxy-Daemon...killing 1265....OK
   Stopping mkeventd...killing 1257......OK
   Stopping mongod...OK
   [root@lsm-server ~]#
   ```

3. Enter:

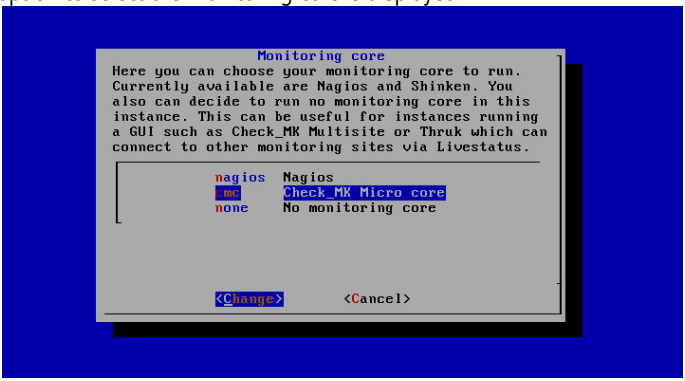
   ```
   [root@<computer name> ~]# omd config lsm
   ```

   The configuration of the LSM site is displayed:

Use the "Tab" or arrow keys to navigate.

4. Select "Basic" and confirm your selection with <Enter>or the return key.
   The following is displayed:

5. Select "Core" and confirm your selection with <Change>or the return key.
   The option to select the monitoring core is displayed.



6. Choose the core, Nagios or Check_MK Micro Core and confirm your choice with <Change> or the return key.

The basic configuration of the selected core is displayed now (in this case: nagios)

7. Return to the "Main menu" and exit the configuration with <Exit>.

   This command line is displayed again

   ```
   [root@<computer name> ~]#
   ```

8. Restart the LSM server:

   ```
   [root@<computer name> ~]#omd start lsm
   ```

   The LSM server is now operating with the other monitoring core.

5 Configuration

The configuration can be performed after installation of the Large Scale Monitor (see section 4 "Installing the Large Scale Monitor"). The software is adapted to the specific local conditions of the network and is configured with different data as regards users, devices and checks.

The side bar contains the snap-in CONFIG – configuration. The configuration options available here can be used to set up a new installation and to extend or change an existing one.

5.1 Overview of the configuration steps

The following is a list of the individual steps of the configuration of the Large Scale Monitor. Use the appropriate links to access the detailed descriptions of the configuration.

	Name	Explanation	Further information
1	**Login**	A web browser is used to access the Large Scale Monitor. A prompt is issued for the user name and password. Generally only user "omdadmin" with password "omd" is created after installation.	See section 3 "The main page"
2	**Creating devices**	The devices to be monitored by the Large Scale Monitor must be made known to the Large Scale Monitor. This is performed manually or with a network scan. The device "lsm-server" is created during the installation and is used to monitor the server.	See section 5.5 "Devices & folders" • Creating devices manually • Creating devices via CSV import • Creating devices by network scan • Creating devices via bulk import
3	**Creating checks**	The bulk discovery identifies all of the possible checks for the configured devices. The number of possible checks can be restricted here. Also, the checks for the "lsm-server" need to be determined and enabled.	See section 5.5.2 "Discovering checks"
4	**Creating folders**	Further substructures (e.g. spatial or organizational) can be defined below the Main directory. In connection with these structures, the access rights (permissions) for users / user groups are assigned.	See section 5.5.8 "Creating folders"
5	**Creating users and groups**	Only one user, administrator "omdadmin", is created on installation. Other users and groups can be created. These are then also assigned different roles.	See section 5.12 "User" See section 5.14 "Contact groups"

6	**Time periods**	Only one time period is created during the installation, the "always" period. You are able to create other time periods here.	See section 5.16 "Time periods"
7	**Device/check parameters (rules)**	Complex sets of rules can be created for devices and checks.	See section 5.9 "Device & check parameters (rules)"
8	**Enter licenses**	The licenses must be entered before (active) monitoring can be started by the Large Scale Monitor.	See section 5.20 "LSM License Management"
9	**Backup & restore**	The configuration can be saved. A saved configuration can be restored if required. A backup (snapshot) is automatically created on activation.	See section 5.19 "Backup & restore"
10	**Activation of the configuration**	After the configuration has been performed, it must then be activated. Only then are the devices and checks 'visible', i.e. they can be displayed in the Large Scale Monitor. A backup (snapshot) is automatically created on activation.	See section 5.4.2 "Activating changes"
11	**Defining views**	The definition of different views is part of the monitoring function within the active Large Scale Monitor.	See section 6 "Display, views"

5.2 Test configuration

If you wish to configure an initial test in which some devices are monitored by the Large Scale Monitor, you have to perform the following steps from the table (see above):

- Login (1)
- Creation of devices (2)
- Creating checks (3)
- Enter licenses (8)
- Activation of the configuration (10)

Only then do real values for the devices appear in the view provided by the Large Scale Monitor.

5.3 Further configuration options

Departures from the standard installation are only required in rare cases. The following settings can be changed or extended in the Large Scale Monitor configuration.

Change device tags	Every device has a number of parameters. The values of these parameters are checked by the Large Scale Monitor. You are able to define these for a device, regardless of the original value. This method can be used when exceptions for certain devices have to be configured.
Global settings	In rare cases it may be worth using values that deviate from the defaults set during installation.
Device groups	Devices are already grouped in a meaningful way when they are created. If a different grouping is required, other groups can be created here.
Check groups	Checks already have meaningful grouping. If a different grouping is required, other groups can be created here.

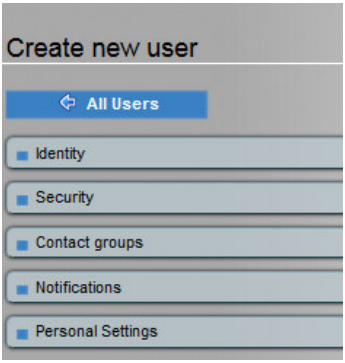
5.4 Main configuration menu

This gives you an overview with brief explanations of the configuration options.

5.4.1 Generalities in the configuration

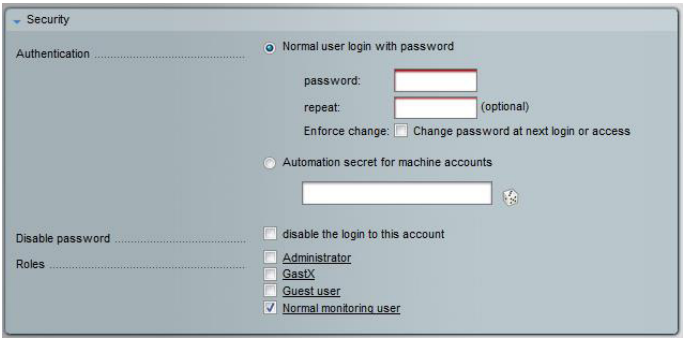
If a unit (device, group, check, user, etc.) is created or modified, different individual areas of the properties are shown on the Properties screen.

Example: Properties of a user



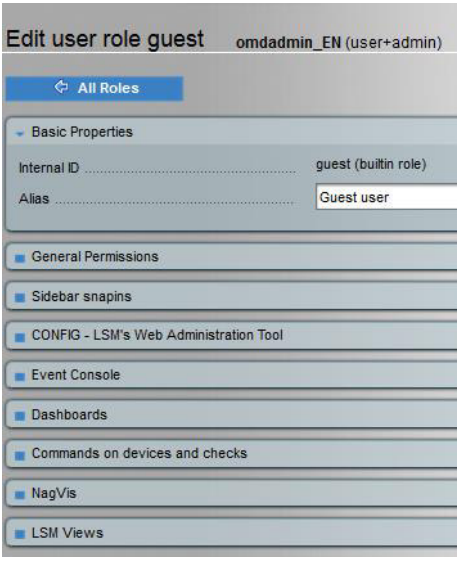
These sections frequently contain multiple options, which can be displayed by clicking one of the sections, such as "Security". Now the individual options in this section can be edited.

Example: Roles of a user



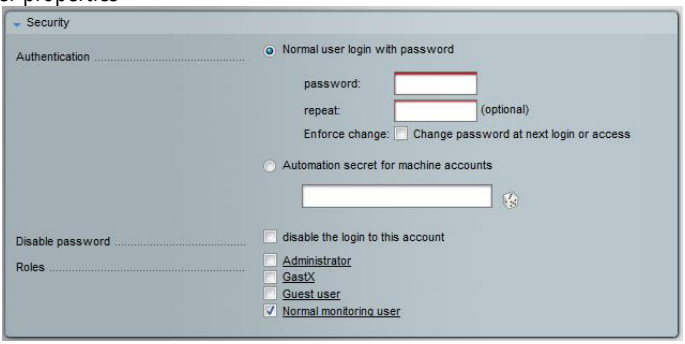
Many options are in turn linked to the Properties screen assigned to them. Clicking these links directly exits the original configuration.

Example: Properties of a role



We recommend that you open the link on a new screen or in a new window. If you make a change there that you also want to save on this screen, this change is also available there after refreshing of the original screen (F5 key).

Example: User properties



➢ NOTE: If you change your mind about creating a user and you did not open another screen or window, you can only return to the original screen with the Forwards/Backwards buttons of the web browser  , and refresh it with F5. Doing this can lead to confusion!

5.4.2 Activating changes

Configuration changes that are not yet activated are displayed in the top left of the main menu (1). These changes currently have no effect on the monitoring.

➢ NOTE: The appropriate licenses must be in place before configuration changes can be activated (see section 5.20 "LSM License Management")

How to activate configuration changes for monitoring:

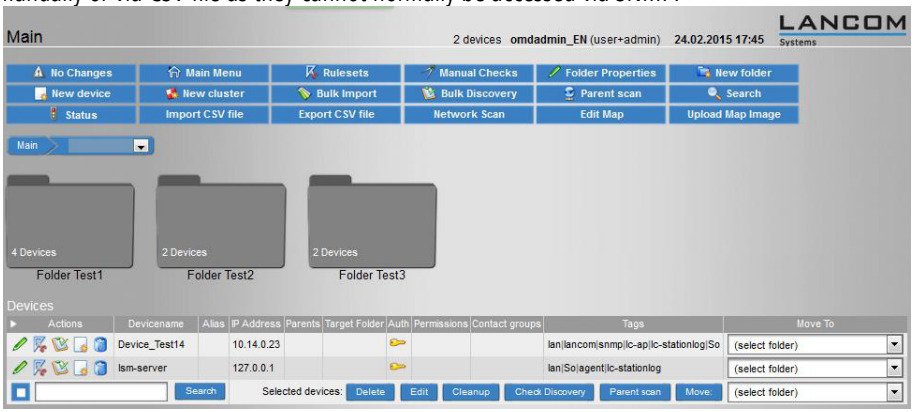
1. To activate configuration changes, click the "Changes" button.
2. An overview of the configuration changes made since the last activation is opened.
3. To activate the changes, click the "Activate changes" button.

➢ NOTE: Configuration changes made cannot be deactivated. They must be undone individually. You can also restore the previous state (see section 5.19 Backup & restore).

5.5 Devices & folders

Here you are able to edit, change and extend the entire structure of the installation, as well as to add and move devices or folders.

Where mobile devices are to appear in the device list or search, they need to be imported manually or via CSV file as they cannot normally be accessed via SNMP.



The button provide quick access to several configuration options:

	Explanation
x changes	This is where you can identify and activate changes that are not activated. Please refer to section "Activating changes" for more information.
Main menu	Shows an overview of all configuration options. For more information, please refer to section 0 " Main configuration menu".
Rule sets	Here you can create and change the rule set of the Large Scale Monitor. For more information, please refer to section 5.9 "104Device & check parameters (rules)".
Folder properties	Specification of the properties of subfolders. For more information, please refer to section "Editing folders".
New folder	Creating a new folder. Please refer to section "Creating new folders" for more information.
New device	Enters a single device into the current folder. For more information, please refer to section "Creating devices manually".
New cluster	This groups multiple devices into a cluster. For more information, please refer to section 6 "Display, views"). New cluster5.5.6 "New cluster".
Bulk import	Enters several devices into the current folder. For more information, please refer to section "Creating devices via bulk import".
Bulk discovery	Identifies the checks for the available devices. For more information, please refer to the section "Discovering checks".
Parent scan	It is possible to search a network for superordinate devices (parents) and to specify these.
Search	The Search function can be used to display devices and device groups in the configuration. See section 5.5.11 "Search function".
Status	The "Status" button is used to display the status of the devices in the currently selected folder. The "All devices" check is run for the selected folder (see section 5.5.5 "Status").
Import CSV file	New devices are imported via a CSV file. Please refer to the section "Creating devices via CSV import" for more information.
Export CSV file	Exports the data of the identified device into a comma-separated file. Please refer to section 5.5.14 "Exporting a CSV file" for further information.
Network scan	New devices are automatically discovered by the system. Please refer to "Creating devices by network scan" for further information.
Edit map	In order to organize devices in a meaningful manner (spatially or organizationally), devices can be placed on an imported map. See section 5.5.13 "Edit map"
Upload map image	In order to organize devices in a meaningful manner (spatially or organizationally), a map can be imported. The devices can then be positioned on this map (see section 5.5.12 "Uploading mapsUploading").

5.5.1 Creating devices

In order to monitor devices, the devices must be known to the Large Scale Monitor. Created devices can be processed at a later time (see section 5.5.3 "Editing devices"). The Large Scale Monitor requires as a minimum the device name, the IP address and the device type. The IP address of a device can be added at a later date, see the section under "IP address".

Device "lsm-server"

During the installation of the LSM, the device "lsm-server" is always created, regardless of the server name specified during the installation (see section "Running the installation"). This device handles the monitoring of the server PC itself, e.g. free RAM or disk space, or whether the licenses are up to date (see "Continuous license check"). This device requires a device license and can be removed, if desired. In this case the server PC is no longer monitored.

For this device, too, after the installation the checks must be determined and configured (see section 5.5.2 "Discovering checks") and then activated (see section 5.4.2 "Activating changes").

Device name

The name is defined when entered. Choose a name that is unique across the system using only letters A-Z and a-z, digits 0-9, hyphens, full stops and underscores. The DNS name is usually selected.

IP address

The IP address can be a numerical IP address (e.g. 10.10.10.241) or a resolvable DNS name.

If the IP address is left empty, the device name is resolved when the changes are activated.

If the monitoring server cannot resolve the name of the device by means of /etc/hosts or DNS, an explicit IP address or a resolvable DNS name for the device can be specified here.

Device type

The device type specifies which type of device it is. A differentiation is made between

- Servers (monitored by agent)

  Windows and Linux servers are monitored with the Check_MK agent. This agent must be installed on the server being monitored (see section 4 "Installing the Large Scale Monitor").

- Devices monitored with SNMP or PING

  Individually you have the choice between:

  - LANCOM WLAN access point
  - LANCOM WLAN controller
  - LANCOM access device/router
  - LANCOM switch
  - Other SNMP device
  - Device using Check_MK agent
  - Use PING only
  - Device using Check_MK Agent+SNMP
  - SNMP v1 Device

  The LANCOM devices monitored (WLAN access point, WLAN controller, access device/router or switch) must at least have read-only authorization for the SNMP protocol.

The devices for monitoring can be imported into the configuration in different ways:

- Manual entry

  Individual devices are entered and identified by their IP address or DNS name. Please refer to the section "Creating devices manually" for more information. If the SNMP community is different to the default "public" setting, the SNMP community must also be changed in the Large Scale Monitor. This needs to be done with the help of a created rule (see section 5.95.9.1 "Device & check parameters (rules)"). You will find an example of this in section 5.9.1 "Example (setting the SNMP community with the help of a rule)".

- Import of a CSV file

  The devices to be imported are listed in a comma-separated file (CSV) with their IP addresses or DNS names. Please refer to the section "Creating devices via CSV import" for more information.

- Network scan

  The entire network (IP address range) is scanned for devices. These are transferred to the configuration and can be edited at a later time. Please refer to the section "Creating devices by network scan" for more information.

- Bulk import

  You can create devices simply by identifying their names in a list. Please refer to the section "Creating devices via bulk import" for more information.

After the devices have been identified by the system, the associated checks can be determined automatically. Please refer to section 5.5.2 "Discovering checks" for further information.

Existing devices can be edited here. Please refer to section "Editing devices" for more information.

After the change to the configuration, the change must first be activated (see section 5.4.2 "Activating changes").

The data for devices identified in the system can be exported to a CSV file. Please refer to section 5.5.14 "Exporting a CSV file" for further information.

Creating devices manually

Individual devices can be made known to the Large Scale Monitor by manually entering the required parameters. Device name, IP address and device type are absolute requirements here.

How to manually add devices

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

   You will find a pre-configured device called "lsm-server". This monitors the server itself.

2. The "New device" button can now be used to include a new device in the monitoring function.

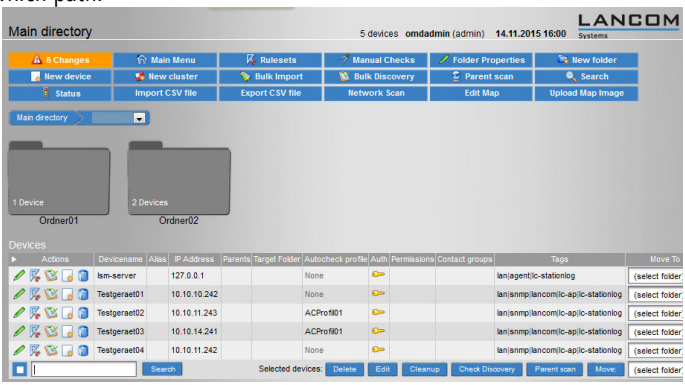
   You must specify at least

   - Device name
   - IP address (optional, can be resolved later)

- SNMP community (optional; public is used by default)
- Device type

3. The "Save & Finish" button creates the new device and it is added to the list of devices.

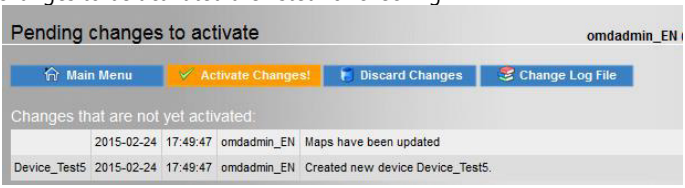
   "Save and go to checks" allows you to directly define checks for the newly created device.
   "Save & test" allows you to establish if the newly connected device can be accessed and via which path.



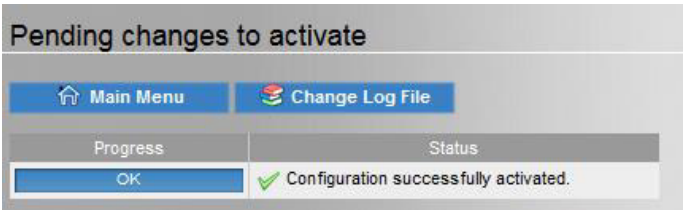
4. More devices can be added in the same way if required.
5. Once all the devices for monitoring are present in the list, the next step is to determine the individual checks for all of the devices by using the "Bulk discovery". Alternatively, you can assign an autocheck profile to the devices. Please refer to the sections 5.5.2 "Discovering checks" and 5.6 "Autocheck profiles" for more information about this.
6. After the bulk discovery, you can display the list of devices again with the "Folder" button.

   All new devices and their configurations are now available in the configuration (CONFIG) area. The number of changes is shown on the "x Changes" button.
7. To make the changes known to the monitoring function, the changes must be activated (see section 5.4.2 "Activating changes").
8. Click the "x Changes" button.

   An overview of the configuration changes made since the last activation is opened.
   The changes to be activated are listed for checking.



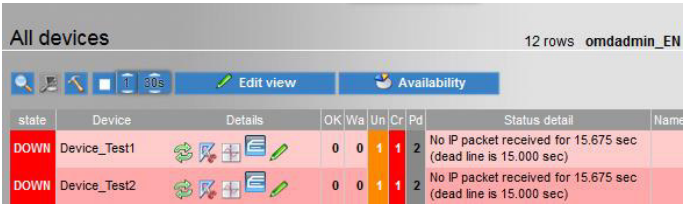
9. To activate the changes, click the "Activate changes" button.



All changes are transferred to the monitoring function.

➢ NOTE: Activation is only possible when a sufficient number of devices are licensed. Activation codes may have to be added in "License Management" (see section 5.20"LSM License Management").

10. The list of monitored devices can be shown in the Large Scale Monitor with the "All Devices" view.



Creating devices via CSV import

If more than one device needs to be connected, it can be worthwhile performing this automatically, for example with a CSV file. Ideally this CSV file is exported from the LANconfig configuration program used to configure LANCOM devices. The format is suitable for importing all of the required information, including the SNMP community. For details on how to export available devices see section 5.5.14 "Exporting a CSV file".

Format of the CSV file

Separator	Individual pieces of information must be separated by a semicolon (;).
Title line	There is a title line
1st column	Contains the directory path.
4th column	Contains the IP address, either numerical or the DNS name.
7th column	Contains the SNMP community.
8th column	Contains the device name.
25th column	Contains device tags (multiple entries are separated by a comma)

➢ NOTE: All devices created via the import of a CSV file are created as access points. If you want to create a server, you can set the device type for the server using "Device using Check_MK Agent" or you can run a network scan (see section "Creating devices by network scan").

How to import devices via CSV file

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

2. You will find a pre-configured device called "lsm-server". This monitors the server itself.
3. You are now able to import multiple devices with the "Import CSV file" button .

4. Select the import file and click "Start".

   After the import, all new devices are included in the list and known devices are simply ignored.
   To discover new devices, proceed from here as described in "How to manually add devices" from step (5).

5. Once all the devices for monitoring are present in the list, the next step is to determine the individual checks for all of the devices by using the "Bulk discovery". Please refer to the section 5.5.2 "Discovering checks" for more information about this. All devices are addressed via SNMP and the checks available for this device are determined.

   Alternatively an autocheck profile can be assigned to these devices (see section 5.6 "Autocheck profiles").

6. Keep the settings ("Find only new checks" and "Include all subfolders") and start the discovery with "Start" . Checks can be aborted at any time.

➢ NOTE: By closing the browser window the bulk discovery is halted.

   An overview is displayed of the devices found and any error messages. You can repeat the process, retry only failed devices, or end the process.

7. After the bulk discovery, you can display the list of devices again with the "Folder" button.

   Currently, all new devices and their configurations are available in the configuration (CONFIG) area only. The number of changes is shown on the "x Changes" button.

8. To make the changes known to the monitoring function, the changes must be activated (see section 5.4.2 "Activating changes").

   - Click the "x Changes" button.
   - An overview of the configuration changes made since the last activation is opened.
   - The changes to be activated are listed for checking.

   All changes are transferred to the monitoring function with "Activate Changes".

➢ NOTE: Activation is only possible when a sufficient number of devices are licensed. Activation codes may have to be added in "LSM License Management" (see section 5.20 "LSM License Management").

Creating devices by network scan

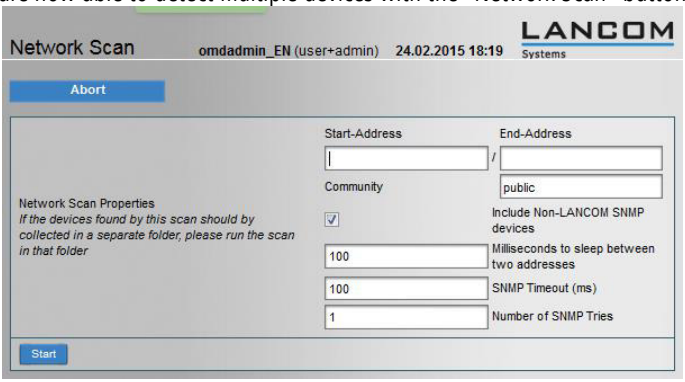
You can also use the automatic discovery of devices in a network. After this type of scan you then still need to specify the individual configuration parameters (check discovery), as with the other methods.

How to create devices with a network scan

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

   You will find a pre-configured device called "lsm-server". This monitors the server itself.

2. You are now able to detect multiple devices with the "Network Scan" button .



3. After entering the start and end IP addresses, and optionally the relevant SNMP community, the scan is initiated with "Start" . Checks can be aborted at any time.

   After the scan, all new devices are in the list and devices already known are ignored.

4. Once all the devices for monitoring are present in the list, the next step is to determine the individual checks for all of the devices by using the "Bulk discovery". All devices are addressed via SNMP and the checks available for this device are determined. Please refer to the section 5.5.2 "Discovering checks" for more information about this.

   Alternatively an autocheck profile can be assigned to these devices (see section 5.6 "Autocheck profiles").

5. Keep the settings ("Find only new checks" and "Include all subfolders") and start the bulk discovery with "Start" . Checks can be aborted at any time.

➢ NOTE: By closing the browser window the bulk discovery is halted.

   An overview is displayed of the devices found and any error messages. You can repeat the process, retry only failed devices, or end the process.

6. After the bulk discovery, you can display the list of devices again with the "Folder" button.

Currently, all new devices and their configurations are available in the configuration (CONFIG) area only. The number of changes is shown on the "x Changes" button.

7. To make the changes known to the monitoring function, the changes must be activated (see section 5.4.2 "Activating changes").
8. Click the "x Changes" button.

   An overview of the configuration changes made since the last activation is opened.
   The changes to be activated are listed for checking.
   All changes are transferred to the monitoring function.

➢ NOTE: Activation is only possible when a sufficient number of devices are licensed. Activation codes may have to be added in "LSM License Management" (see section 5.20 "LSM License Management").

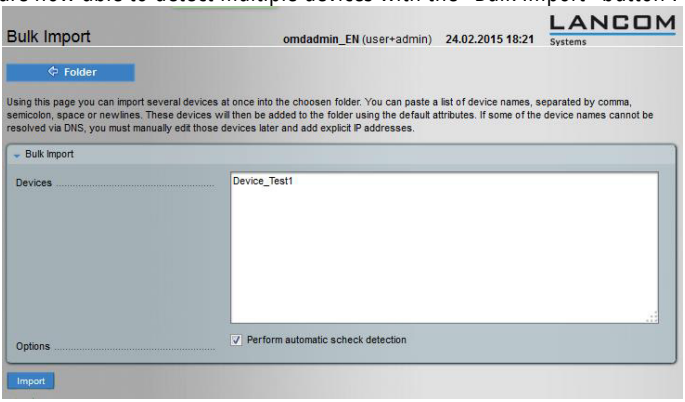
Creating devices via bulk import

You can also import several devices together. In doing so you enter a list of the device names.

How to create devices via bulk import

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

   You will find a pre-configured device called "lsm-server". This monitors the server itself.
2. You are now able to detect multiple devices with the "Bulk Import" button .



3. Enter the device names into the "Device" field, separated by commas, semi-colons or line breaks. The devices are added with the default attributes defined for this folder. (See section 5.5.9 "Editing folders" to do this).
4. If you would like to automatically discover the checks, enable the "Perform automatic check detection" option.
5. Click on the "Import" button to start the process.

If you have enabled the bulk discovery, the parameters for the discovery check are queried first (see the section "Parameters for the bulk discovery").
All stated devices are created in the current folder.

5.5.2 Discovering checks

When new devices are identified in the system, the checks supported by each of the devices can be automatically detected (discovered) at a later time after the purely nominal identification of the devices. This process is started with the help of the bulk discovery. All useful checks are listed for each device, i.e. all checks providing information about this device.

Select the bulk discovery if multiple new devices are to be identified. A variety of parameters can be set for these checks. All devices are addressed via SNMP or the agent according to their device type, thereby determining the checks available for this device.

Discovering checks for a single device

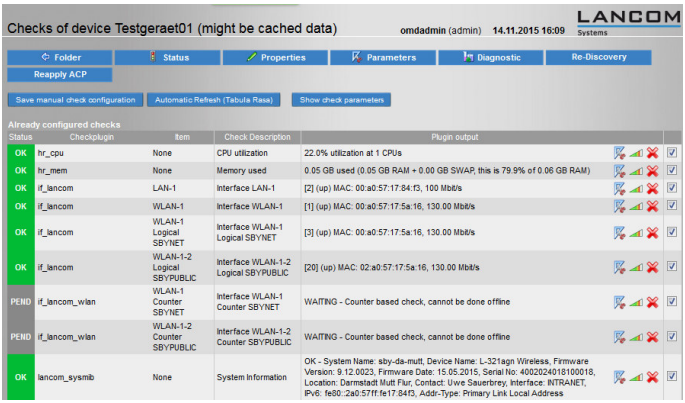
It is also possible to check a single device with the help of a bulk discovery. Following the installation, the device "lsm-server" runs to constantly monitor the server PC and check the license. The checks for this device also need to be discovered and enabled.

How to discover the checks for a single device

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

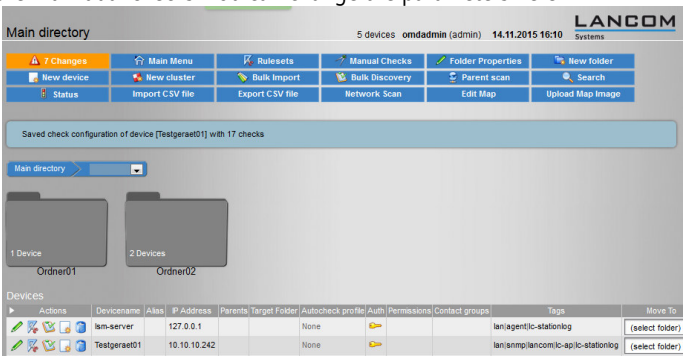
   You will find a pre-configured device called "lsm-server". This monitors the server PC.

2. Click the icon  of the device for which the checks are to be discovered; this opens the page with the checks for this device (in this case: lsm-server).



You have several options:

- You can configure all of the discovered checks with the button "Activate missing".
- If you only want to find a small number of checks, you can select these using the check boxes on the right-hand side and then clicking "Save manual check configuration".
- With "Automatic refresh" you can discover all of the available checks again.
- The button "Show check parameters" gives you a detailed view of the parameters of the individual checks. You can change the parameters here.



3. Configure the checks according to your needs.
4. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

Bulk discovery

When the checks for a device are discovered for the first time, the check detection is added by default. This check is made at extended intervals and determines whether there are new checks for this device.

For very large installations, it is possible to bypass this time-consuming discovery process with the help of autocheck profiles. Please refer to section 5.6 "Autocheck profiles" for further information.

Parameters for the bulk discovery

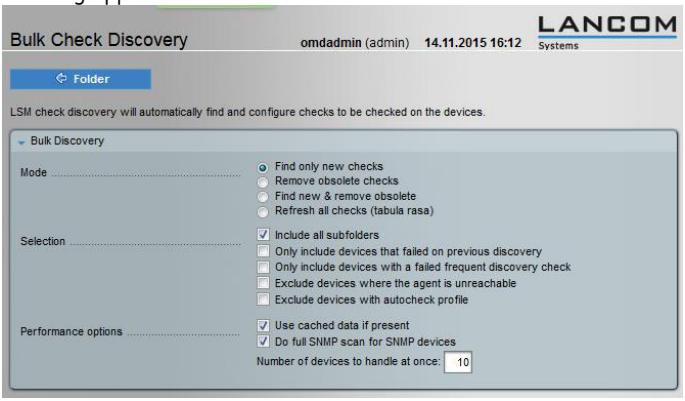
Mode	• Find only new checks Checks already in the system are not considered. • Remove obsolete checks There is no search for new checks. • Find new and removed obsolete checks Data already collected about this check is retained. • Refresh all checks (tabula rasa) Data previously collected is deleted.
Selection	• Include all subfolders • Only include devices that failed on bulk discovery. • Only consider devices for which a regular bulk discovery detected new checks. • Exclude devices whose agent cannot be accessed. • Exclude devices with autocheck profile
Performance options	• Used saved data, if available • Perform full SNMP search for SNMP devices. • Number of devices handled at once.

How to perform a bulk discovery

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration", for example in the side bar on the main page.

2. Click on the "Bulk Discovery" button in the folder view or, if applicable, you have selected the discovery of the checks for several devices in the Bulk Import.

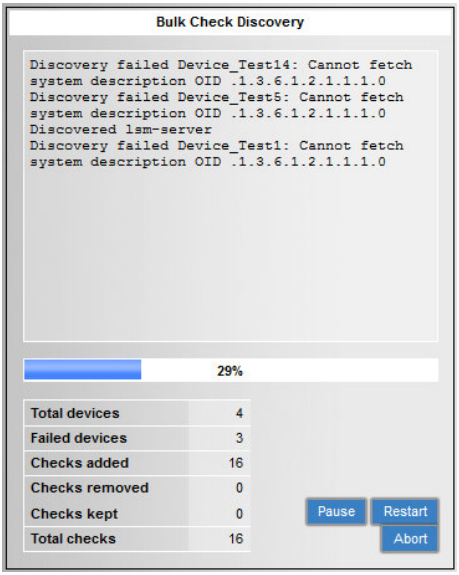
   The following appears



3. After creating devices anew, keep the settings ("Find only new checks" and "Include all subfolders") and launch the bulk discovery with "Start" . Checks can be aborted at any time.

   All of the devices that have been set with an autocheck profile can be excluded from the discovery here. This speeds up the discovery process.

➢ NOTE: By closing the browser window the bulk discovery is halted.



An overview is displayed of the devices found and any error messages. You can repeat the process , retry failed devices or end the process .

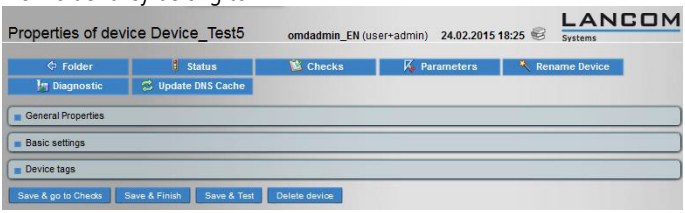
4. After the bulk discovery, you can display the list of devices again with the "Folder" button.

   All new devices and their configurations are now available in the configuration (CONFIG) area. The number of changes is shown on the "x Changes" button.

5. To make the changes known to the monitoring function, the changes must be activated (see section 5.4.2 "Activating changes").

5.5.3 Editing devices

You can edit devices that already exist at any time, i.e. you can change their properties and, in particular, which folder they belong to.



There are also a number of quick-access editing options via the buttons here:

Folders	Change back to the device view in this folder.
Status	Displays the device's status (see section 5.5.5 "Status")
Checks	Displays the possible checks for this device.
Parameters	Displays the monitoring parameters configured for this device.
Rename device	Here the device name displayed on the interface can be changed. The internal name remains unchanged.
Diagnosis	This allows you to spontaneously test the device's connections (see also section "Diagnosis").
Update DNS Cache	Updates the IP addresses of all devices, primarily those identified by their device name because the IP address remained empty when created.

Device properties

When creating a device you only need to define the name, IP address (optional) and device type. The checks are discovered. One device may have multiple properties. These can also be configured later on. User-defined device tags (attributes) must already have been created (see section 5.7 "Device tags (device attributes)".) Only the default tags are explained here.

If device properties are not explicitly set out then these devices can inherit these properties later

from your folder (see section 5.5.10 "Inheritance of properties").

General properties	
Name	**Device name** Make sure that the name is descriptive.
Basic settings	
Permissions	You can only assign permissions to members of contact groups. These users can configure this device. It makes more sense to configure the permissions via folders.
SNMP Community	Enter the SNMP password for this device here.
Parent element	Enter the name of a parent device here (See also section 5.5.7 "Parent scan")
Target folder	Displays the folder with CSV file import (for information).
Autocheck profile	Displays whether and, if so, which autocheck profile has been set for this device (see section 5.6 "Autocheck profiles").
Device tags	
Device type	The device type is specified when setting up a device (see for example "Creating devices manually") • LANCOM WLAN access point (default) • LANCOM WLAN controller • LANCOM access device/router • LANCOM switch • Other SNMP device • Device using Check_MK agent • Use PING only • Device using Check_MK Agent+SNMP • SNMP v1 Device
Station log	**Station history** A chronological log is recorded of the WLAN stations which log on to access points. The transmission of these logs takes up bandwidth. This item specifies whether the Large Scale Monitor can use this log for monitoring (default) or not.
Network connection	**Network connection** • LAN – short PING times (default) • WAN – long PING times • WWAN – extra-long PING times
Monitoring	**Monitoring** This item specifies whether the device can be monitored (default) or not.
SNMP Bulkwalk	The SNMP devices are checked as a bulkwalk (efficient collective check).

How the properties of a device are changed

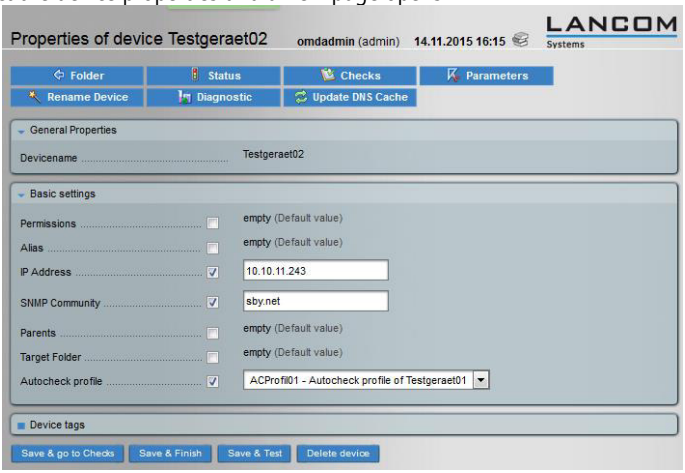
1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

The "Devices" table lists all of the devices assigned to this folder (here: Main directory).

2. Here you can

- edit the device properties 
- delete an existing device 
- create a new device by copying an existing one  .
- edit the rules for this device  .
- edit checks for this device and perform a bulk discovery  .

3. Select the device properties and a new page opens.



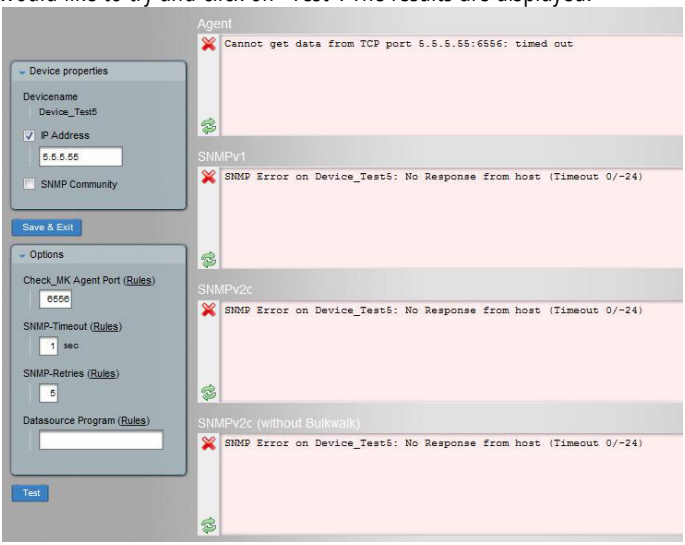
4. Set any desired properties here or leave the default settings. These can be subsequently overwritten by parents.
5. Complete your entries.

- You can "Save and Finish" your changes.
- "Save & go to checks" opens the list of checks for this device.
- "Save & test" starts a new connection test (see section "Diagnosis").

6. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

Diagnosis

You can test the connections for a device spontaneously. To do this, open the "Diagnosis" dialog in the device properties. This allows you to test the connection to a device directly. You can either test the current connection data or even try out alternatives. Just configure the options you would like to try and click on "Test". The results are displayed.



5.5.4 Moving the devices

If devices have been imported into the system, they should then be transferred to the structure. The structures must first be created for this. If the appropriate folders have been created and configured, the imported devices can be moved to them.

How to move devices into new destination folders

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. Select the folder that contains the devices to be moved.

3. The displayed devices can then be moved to the destination folder.
   - You can move a single device by selecting the new destination folder from the "Move To" column. The device is moved instantly.
   - You can use the check boxes (1st column, where enabled with) to select multiple devices. In the lowermost line, select a destination folder for all devices selected click on "Move".

5.5.5 Status

During configuration, you can use the "Status" button or the icon at any time to show the state of the devices in the current folder. The "All devices" check is run for the selected folder (see section 6 "Display, views").

5.5.6 New cluster

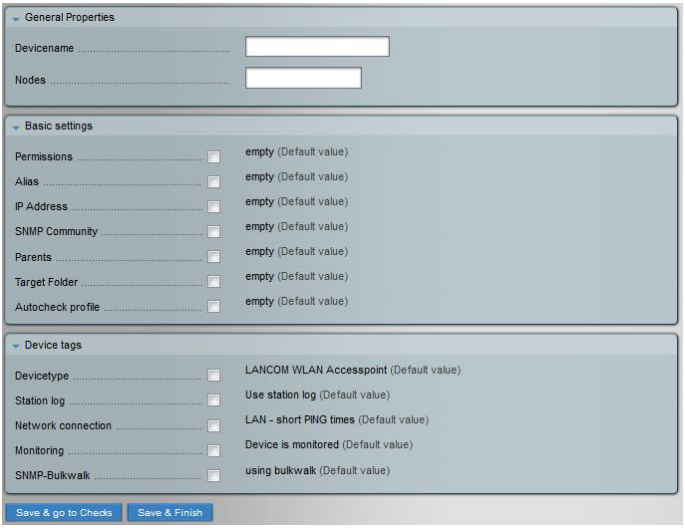
Multiple devices can be collected into a "cluster". The Large Scale Monitor then treats these as a single device. If checks sent to this cluster are to query more than just its accessibility, then the devices contained in this cluster should be of the same type. Otherwise more detailed checks simply make no sense.

It is possible to create a cluster (with at least one device) and to add further devices later.

How to create a new cluster

Requirement:
The devices that are to be collected here must be known to the system already (see 5.5.1 "Creating ").

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. Select the button "New cluster".



3. Enter the name of the cluster.
4. Under "Nodes" you can specify all of the devices for this cluster.
5. Define the properties of the cluster here.
6. With "Save & Finish" you conclude the configuration of the cluster. Selecting "Save & go to checks" allows you to directly edit the checks for this new cluster.
7. The new cluster  is now included in the list of devices (e.g. under the view "All devices").

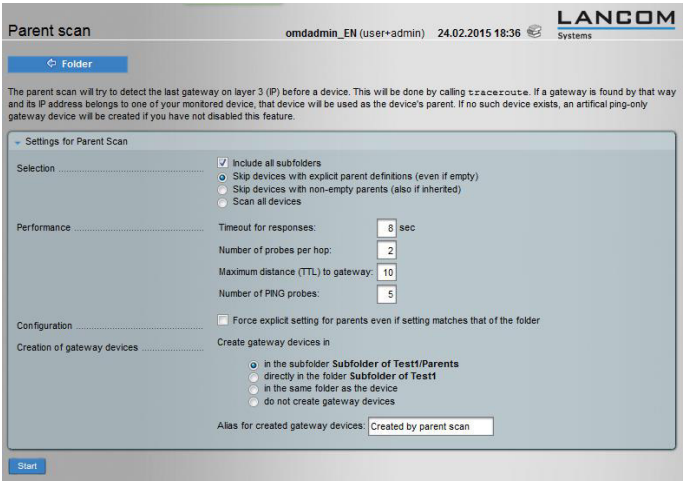
5.5.7 Parent scan

It is possible to search a network for parent devices and to set them.

- by specifying a parent in the device properties
- By inheriting from a folder. Each device inherits the properties of the folder containing it.
- By searching the network. If no parent has been specified, then the gateway nearest to the device on layer 3 is taken to be the parent.

How to search for parent devices

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. Select the button "Parent scan".



3. Enter criteria for the following search:
   - Selection:
     - Select the check box if you want to include all subfolders.

       You can exclude devices from the search:
     - Skip devices for which a parent is already specified in the properties of the device. (This also applies if an empty field has been used explicitly).
     - Skip devices for which a parent is specified, also if it was inherited.
     - Scan all devices.
   - Performance
     - Timeout for responses

Time in seconds to wait for a response from the parent device (default: 8 sec.).

- Number of tests per HOP

  Number of attempts per hop (default: 2)

- Maximum distance (TTL) to gateway

  Maximum distance, measured in hops, to a gateway that is to be set as the parent (default: 10).

- Number of PING attempts

  Specifies the maximum number of PING attempts (default: 5).

- Configuration

  By activating this check box you force the parent to be set for this device, even for those that have already inherited a parent from the folder.

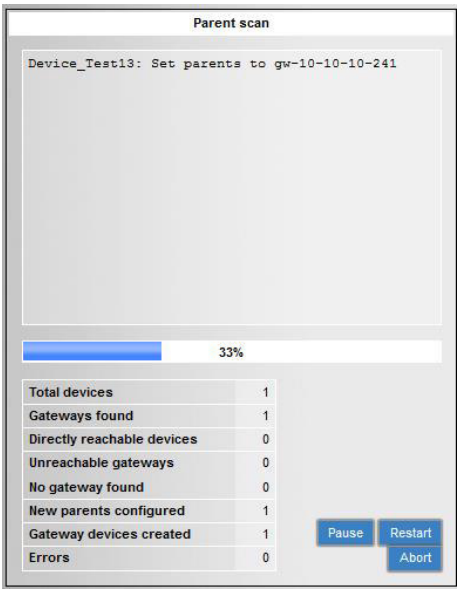
- Creating gateway devices

  The parents that are found (see above) can be newly created as gateway devices:

  - In their own subfolder "Main directory/parents"
  - - Directly in the main directory
  - - In the same folder as the device
  - - No gateway devices created

You can also make a note in the alias text box about how these gateway devices were created ("Created by scan").

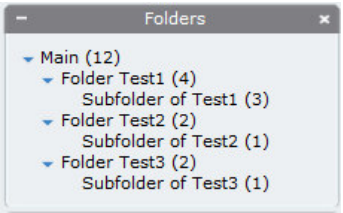
4. Click on "Start" to initiate the search. You can interrupt the search with "Pause", start again with "Restart", or cancel it with "Abort" .



5. Conclude the search with "Finish" .
   The list is displayed with all of the devices in the folder that was searched.

5.5.8 Creating folders

The devices in the system can be structured by organizing them in different folders and subfolders.



These folders can reflect a spatial structure of the network (e.g. Dortmund, Aachen, Berlin), an organizational structure (e.g. Sales, Marketing, Management Board) or a mixture of both (e.g. Sales in Aachen, Marketing in Berlin).

Creating new folders

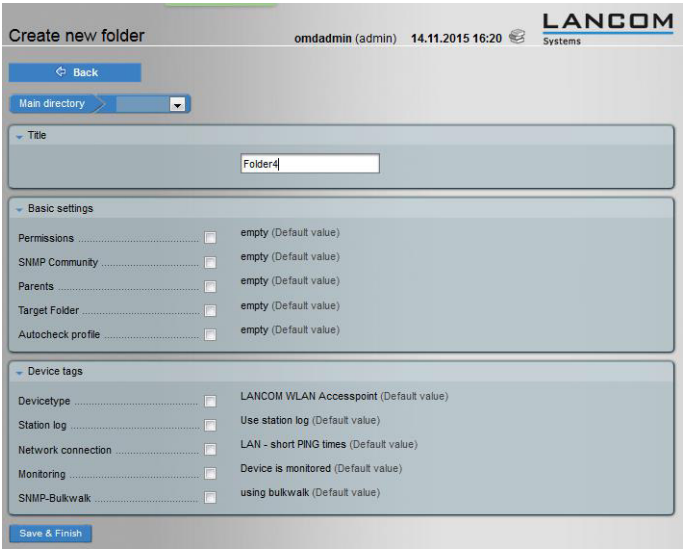
Create folders to organize and manage the devices.

How to create a new folder

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

   You will find a pre-configured device called "lsm-server". This monitors the LSM server itself.

2. Use the "New folder" button to create a new folder.



3. Enter at least the name of the folder.
4. Define the properties of the new folder here. Please refer to section 5.5.9 "Editing folders" for more information.
5. Confirm your entries with "Save & Finish".The newly configured folder will be created.

5.5.9 Editing folders

Each folder has certain properties; the name, the rights, and properties that make no sense for a folder itself, such as the device type. These properties are passed down to the devices contained in the folder.

User-defined device tags must already have been created (see section 5.7 "Device tags (device attributes)".) Only the default tags are explained here.

If folder properties are not explicitly set out then these folders can inherit these properties later from your parent folder (see section 5.5.10 "Inheritance of properties").

Title	
Name	**Name of the folder** Make sure that the name is meaningful and unambiguous.
Basic settings	
Permissions	You can only assign permissions to members of contact groups. These users can then configure the current folder. Additionally, these users can see this folder in the "Structure" snap-in, provided that it is enabled here (option "Add these groups as contacts (in all subfolders) to all devices in this folder").
SNMP Community	Enter the SNMP password for all SNMP devices in this folder. This setting is ignored for devices not using SNMP.
Parent element	Enter the name of a parent device here (See also section 5.5.7 "Parent scan")
Target folder	Displays the folder with CSV file import (for information only).
Autocheck profile	Displays whether and, if so, which autocheck profile has been set for this folder (see section 5.6 "Autocheck profiles").
Device tags	
Device type	The device type is specified when setting up a device (see for example "Creating devices manually") • LANCOM WLAN access point (default) • LANCOM WLAN controller • LANCOM access device/router • LANCOM switch • Other SNMP device • Device using Check_MK agent • Use PING only • Device using Check_MK Agent+SNMP • SNMP v1 Device

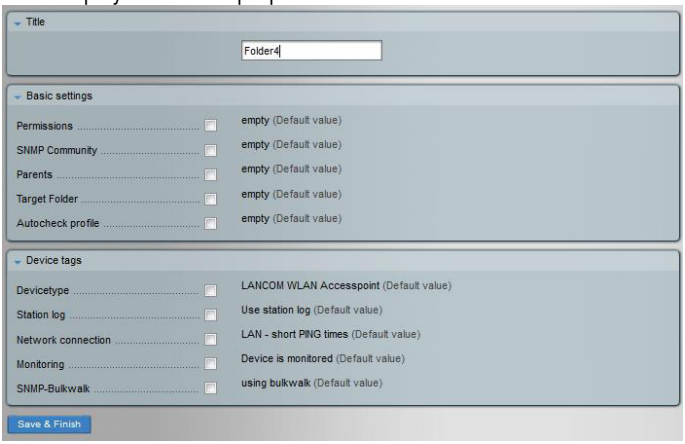
Station log	**Station history** A chronological log is recorded of the WLAN stations which log on to access points. The transmission of these logs takes up bandwidth. This item specifies whether the Large Scale Monitor can use this log for monitoring (default) or not.
Network connection	**Network connection** • LAN – short PING times (default) • WAN – long PING times • WWAN – extra-long PING times
Monitoring	**Monitoring** This item specifies whether the devices can be monitored (default) or not.
SNMP Bulkwalk	The SNMP devices are checked as a bulkwalk (efficient collective check).

How to edit the properties of a folder

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. Select the folder in the sub-title line.

3. Select the "Folder properties" button .

   A window displays the folder properties.



4. Define the properties of the folder here. Please refer to the table above for further information. The folder properties set here are inherited to the subfolders and to the devices contained therein.
5. Confirm your entries with "Save & Finish".

A list of all the devices contained in this folder is displayed.
The new properties of the folder are now configured.

6. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

5.5.10 Inheritance of properties

The folder properties allow device properties to be specified, which are passed down to this folder and then to the devices contained therein.

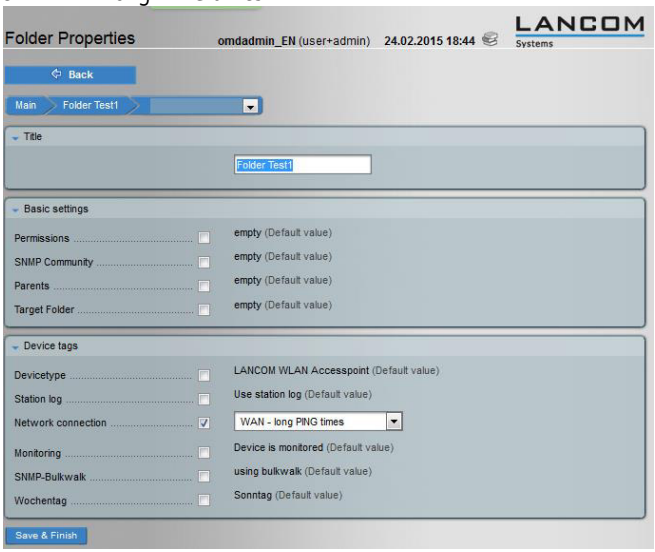
If a property has been explicitly set for a device or folder, then this is also assigned to it. If this allocation is not explicitly selected, then the device or folder (as applicable) "inherits" this property from its folder or parent folder respectively. This inheritance can be identified in the properties (see above)

Example:

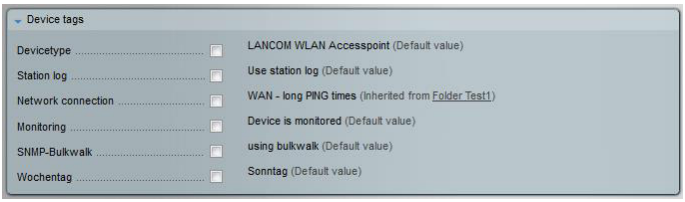
Select "Devices & Folders" in the "CONFIG – Configuration" snap-in on the side bar on the main page, and the subfolder (here: folder test 1)

Open the properties with "Folder Properties".

The example folder "folder test 1" has the property "Network connection" with the value "WLAN - long PING times".



A device in this folder is then given the value "WLAN – long PING times" with a note saying "Inherited from folder test 1" displayed in its properties under "Network connection".



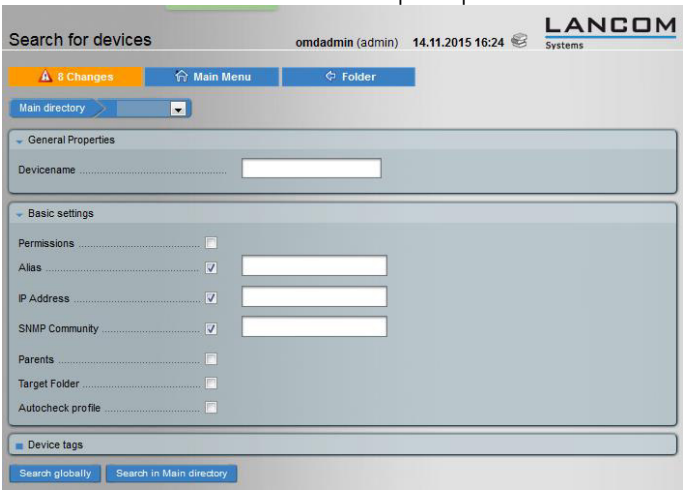
The folder name (here: Test 1 Folder) is linked directly to the folder properties.

5.5.11 Search function

The Search function can be used to display devices and device groups in the configuration.

How to search for devices

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. Select the button "Search". The search mask opens up.



3. Enter the search criteria.

   You have the option of searching the current folder with "Search in..." or all folders with "Search globally".
4. A list is displayed of devices that meet the search criteria.

5.5.12 Uploading maps

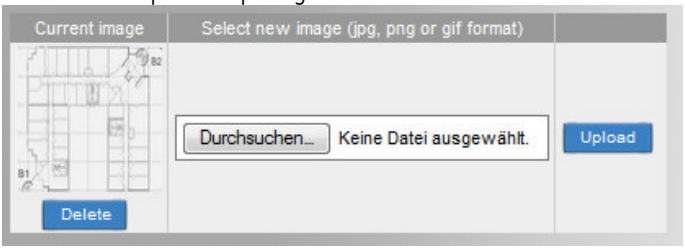
In order to organize devices in a meaningful manner (spatially or organizationally), a map can be imported. When being assigned to a folder, the devices appear on the left-hand edge of the map and can then be positioned. The map can be uploaded to the system as an image in the formats JPEG, PNG or GIF. A map can be created for each individual folder, and the map is a folder property.

► The maps have no effect on monitoring but they facilitate the configuration. Thus changes to the map do not have to be subsequently activated.

How to upload a map

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. Select the folder for which a map is to be imported.

3. Select the button "Upload map image".



4. Use the "Browse..." button and select a file (format: (PNG, GIF or JPEG) that you want to import as a background.
5. Start the import with "Upload".
6. A miniature appears after a successful import.
7. You can use the "Delete" button to delete the map, or upload another one.

5.5.13 Edit map

With a map stored in a folder, the devices that are associated with this folder can be positioned on the map.

How to position devices on a map

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. Select the folder with the devices that are to be positioned on the map.

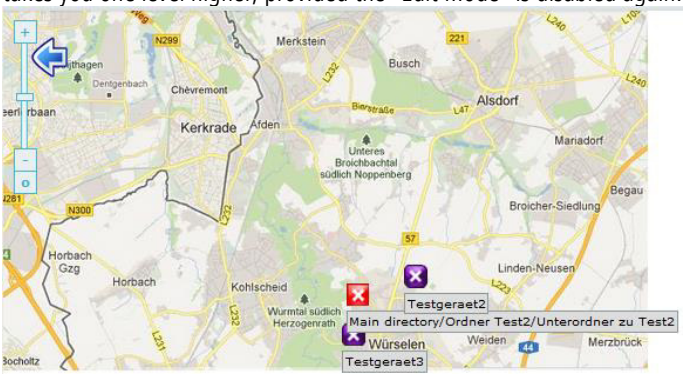
3. Select the button "Edit map".

   The map view opens up. All of the relevant devices are located on the left.

4. In order to move the devices, go to the title bar and then "Edit map" in the menu and select the entry "Lock/Unlock all".

"Edit mode!" is displayed in red in the title bar in the outside right. The devices can now be positioned on the map by drag & drop.

takes you one level higher, provided the "Edit Mode" is disabled again.



5. Conclude the positioning of the devices by accessing the menu "Edit map" again and select the entry "Lock/Unlock all".

   You can now view the map for a folder at any time by clicking on the "Map" button . Each of the displayed devices shows a tool tip when you hover over it with the mouse. If you click on a device, then the full view for this device is displayed.

5.5.14 Exporting a CSV file

It is possible to export the devices saved to a folder and its subfolders to a comma-separated file.

Format of the CSV file

The format of the exported data corresponds to that of the data to be imported. This allows you to export the devices and immediately import them again, for example into another server.

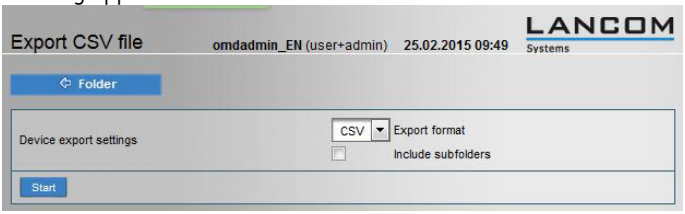
Separator	Individual pieces of information must be separated by a semicolon (;).
Title line	There is a title line
1st column	Contains the directory path.
4th column	Contains the IP address, either numerical or the DNS name.
7th column	Contains the SNMP community.
8th column	Contains the device name.
25th column	Contains device tags (multiple entries are separated by a comma)

How to export devices to a CSV file:

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

2. Select the folder from the device data is to be exported and click on the "Export CSV file" button.

   The following appears



3. Select the format (currently CSV available only). Enable this option if you would like to include devices in the subfolders.
4. Start the export with "Start". Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.
5. The file is saved to the web browser's download directory under the file name hosts-<folder name>-<date and time yyyy-mm-dd_hh-mm-ss>.csv.

The file exported here can immediately be imported again, for example in the event of a server change. Please refer to the section "Creating devices via CSV import" for more information about importing.

5.6 Autocheck profiles

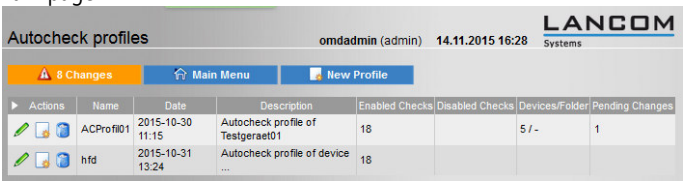
For installations with many of the same devices, the normal discovery of checks is a lengthy process because communications are carried out with each individual device via the SNMP protocol.

Creating an autocheck profile simplifies this process. This involves identifying the checks for one device. This device is then used as a template for all of the other similar devices, i.e. the checks discovered once are carried out for all devices.

How to define an autocheck profile

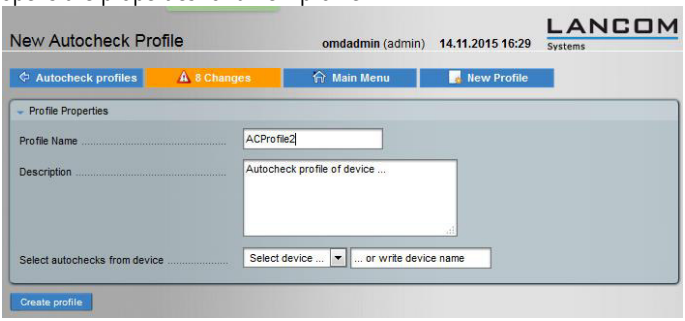
Requirement: You need to have at least one device that can serve as a template for all of the other devices.

1. Select "Autocheck profiles" in the "CONFIG – Configuration" snap-in on the side bar on the main page.



2. Click on the "New profile" button to create a profile.

   This opens the properties for a new profile.



3. Enter a meaningful name here, and use the description to note which device is serving as the template.
4. Then select from the list the device that serves as a template. Alternatively, you can enter the name of the device here.
5. Conclude the profile configuration by clicking on "Create profile".

The autocheck profile has now been created and can be applied to devices.

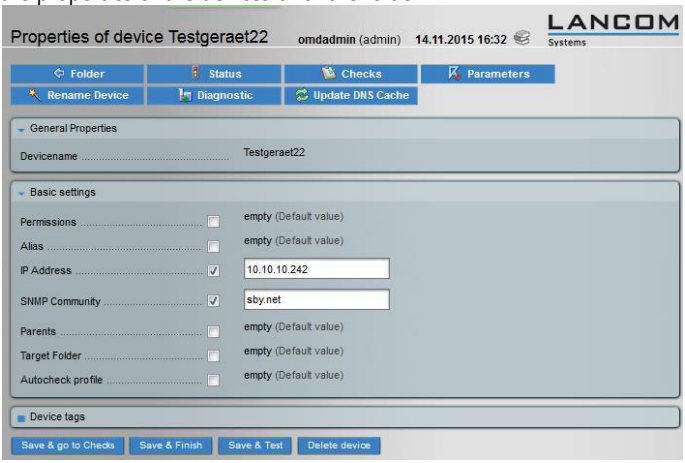
If an autocheck profile has been created, you can use it for additional devices when you create these. This avoids the time-consuming bulk discovery of checks for individual devices. If devices have been set up already, an autocheck profile can be assigned to them by

- editing the device properties,
- assigning the autocheck profile to their folder, or
- assigning the autocheck profile to a parent folder (inheritance).

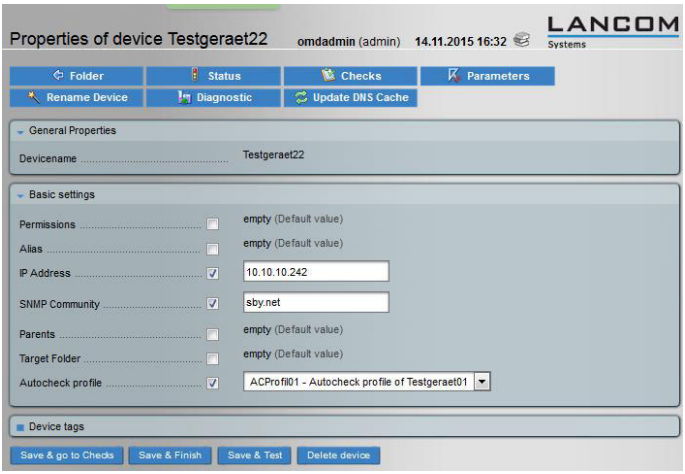
How to apply an autocheck profile

1. Select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

2. Select the devices or select the folder containing all of the devices to be assigned this autocheck profile.
3. Edit the properties of the devices or of the folder.



4. In the basic settings, choose an autocheck profile from the list.



5. Close the configuration with "Save & finish".

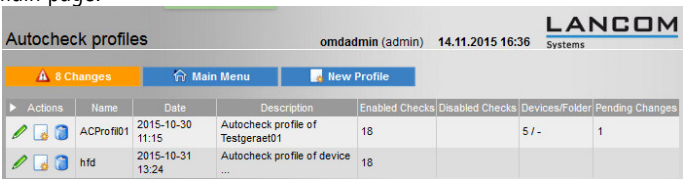
   The autocheck profile has been assigned to the selected devices or folder.

6. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

   As soon as the changes are activated, the checks are carried out according to the autocheck profile for these devices. This effectively makes bulk discovery obsolete.

How to edit an autocheck profile

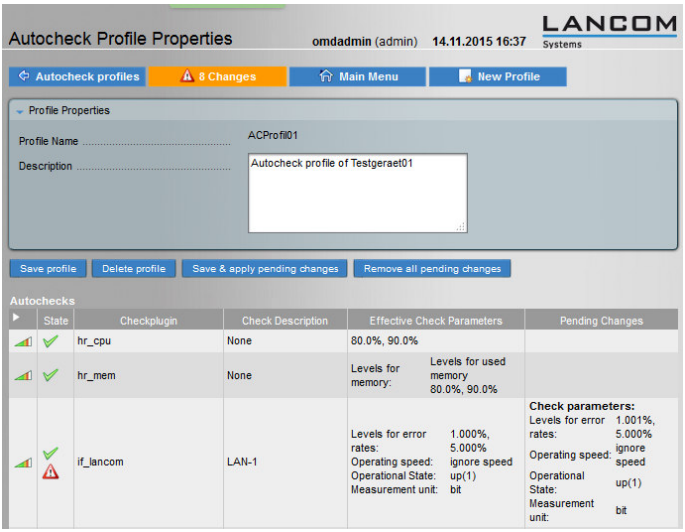
1. Select "Autocheck profiles" in the "CONFIG – Configuration" snap-in on the side bar on the main page.



2. Here you can

   - edit the properties of the profile  or
   - delete an existing profile  . First make sure that the profile is no longer used.
   - create a new profile by copying an existing one  .

3. Select the profile properties and a new page opens.



4. At the top you can edit the description. All of the checks in this profile are listed in the lower part.

   The check properties are opened by clicking the icon for the check. Here, you can change the parameters of each check, or you can disable the check.
   Conclude the editing of your check parameters with "Save".
   The autocheck profile properties are displayed again. The list of the checks shows any changes marked with .

5. You can now use the buttons to

   - save the modified profile,
   - delete the profile,
   - execute the checks with edited parameters with "Save & apply all pending changes" or
   - delete all pending changes. In this case the autocheck profile retains its original form.

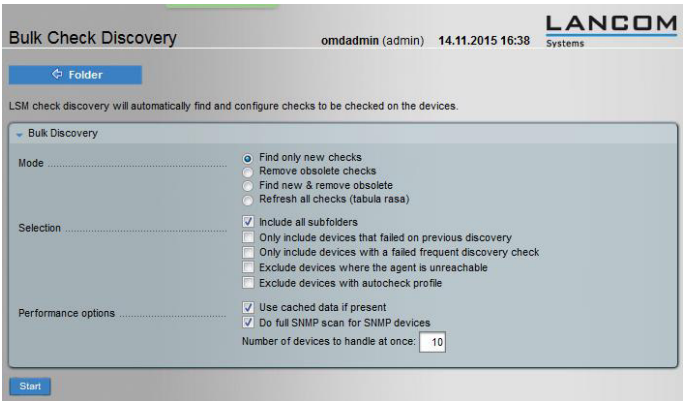
Applying an autocheck profile to different devices

An autocheck profile can be applied to different devices. This is done after an autocheck profile has been assigned by starting a one-off bulk check discovery, which does **not** skip the devices with an autocheck profile. The checks of the differing devices can then be individually edited later.

How to create checks for different devices on the basis of an autocheck profile

1. Start the bulk check discovery and do **not** exclude devices with an autocheck profile.

➢ Please consider that the bulk check discovery can take a very long time if you have a very large number of devices.



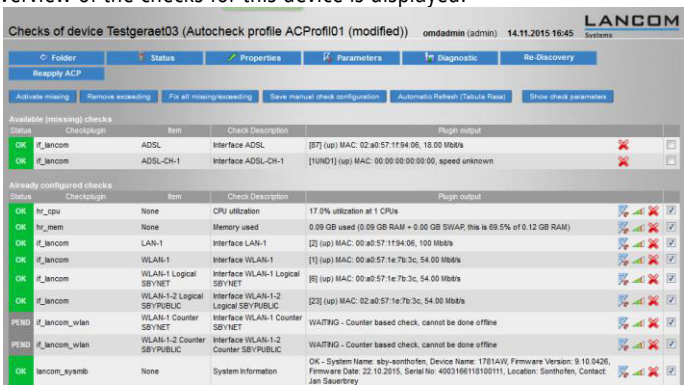
The autocheck profile was created on the basis of a particular device. All of the devices that differ from this are included in the Differences check list (e.g. warnings, unknown).

2. To edit the checks of a device, select "Devices & Folders" in snap-in "CONFIG – Configuration" in the side bar on the main page.

3. Open the properties of a device  .

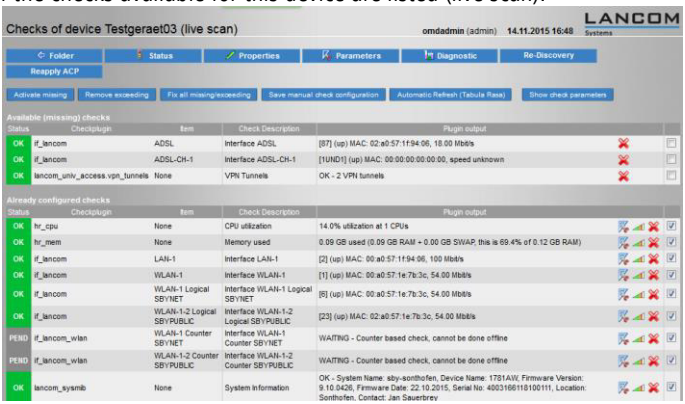
4. Click the "Checks" button.

   An overview of the checks for this device is displayed.



5. Click on "Re-discovery" and allow all of the possible checks for this device to be discovered, as the autocheck discovery may not find all of the checks for this device.

   All of the checks available for this device are listed (live scan).



6. You have a number of options for configuring the individual checks for this device:

- You can use "Activate missing" to enable all non-active checks
- In the right-hand column, activate the check boxes if you only want to activate a selection of the available checks. Save this manual check configuration.
- With "Remove exceeding" you can delete requests that are not available for this device.
- You activate all the missing checks and remove the surplus ones all at the same time.
- With "Automatic refresh (tabula rasa)", you can create a completely new configuration and at the same time retain the autocheck profile.
- You can view the detailed check parameters and if necessary modify them here.

Any changes made still need to be enabled (see section 5.4.2 "Activating changes").
The device that is individually configured in this way continues to have an autocheck profile, so it is excluded from the bulk discovery. The list of checks is marked "Autocheck profile <name of profile> (modified)".

Restoring an original autocheck profile

If a device or folder has an individual check profile that is based on an autocheck profile, the list of checks is marked "Checks of device <Name> (Autocheck profile <Name of profile> (modified))".

To restore the original autocheck profile, click the button "Reapply ACP". All manual changes are deleted and the configuration is returned to its original autocheck profile.

5.7 Device tags (device attributes)

System-wide, you can specify attributes (tags) for devices or folders, and you can set additional attributes (auxiliary tags).

The possible values of an attribute are set when defined and can be extended at any time. If an attribute has just one value, then the attribute is represented as a check box. The default value is a non-enabled check box. If an attribute has multiple values, these are presented as a drop-down list. The top entry is the default value.

The number of possible values is displayed in the column "Choices" in the overview of the device attributes.

A typical attribute can only have one value.

Example:

> The attribute is the "Network connection".
>
> Possible values: "LAN – short PING times", "WAN – long PING times" or "WWAN – extra-long PING times". A list with three options appears with the default value of "LAN – short PING times".

You can also set the order in which the attributes of a device or folder are listed.

Auxiliary tags

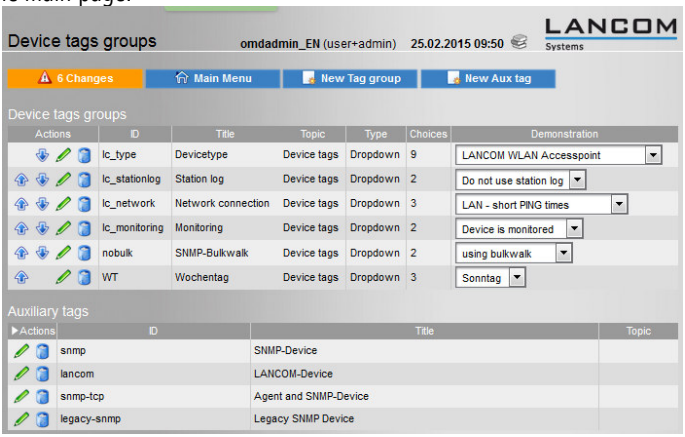
Auxiliary tags are additional attributes assigned to a device if the device tag has the corresponding value.

Example:

> The "weekday" attribute has the values "Sunday", "Saturday" and "workday". The "LANCOM device" check box is enabled for workday. If the device now has the "weekday" attribute set to the value "workday", it also receives the attribute "LANCOM device". If it has the values "Saturday" or "Sunday", it has no auxiliary tag.

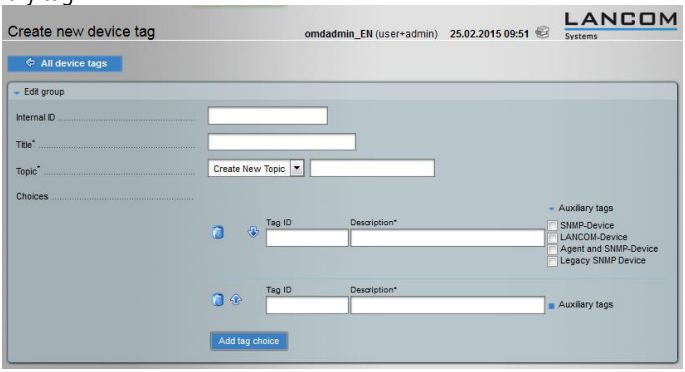
How to create a new device tag

1. Select the entry "Device Tags" in the "CONFIG – Configuration" snap-in on the side bar on the main page.



An overview of the existing device tags and auxiliary tags opens up.

2. Select the button "New device tag" to create a device tag or "New aux tag" to create an auxiliary tag.



3. Enter the parameters required for a device tag.

- Internal ID

  Assign a unique internal name for identification. The characters a-z, A-Z, _ and - are allowed. You can only enter the ID when you create a tag, it remains the same thereafter.

- Title

  This title will later appear everywhere as a tag. Enter a descriptive name here.

- Choices

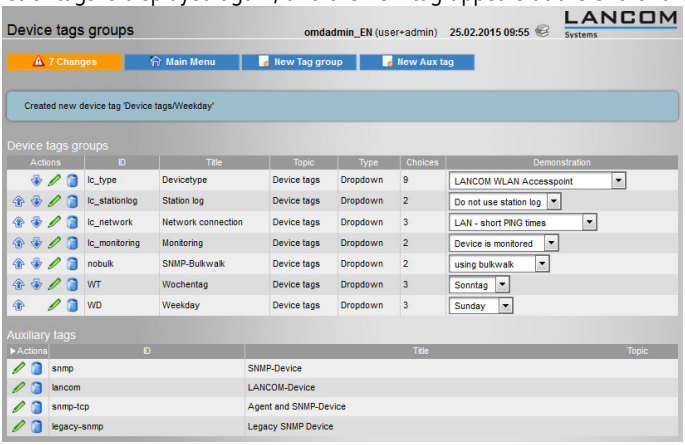
  Enter an identifier (which will subsequently not be visible) and a value for this tag. To specify the different values, click on the button "Add tag choice", specify an ID and enter a meaningful description for each one. This description will appear when selecting this tag from a drop-down list. If you need to set another value in addition to the value of the attribute, you can do this with the aid of the "Auxiliary tags" list.

Example:

If you set the attribute with the tag "lc-switch" (LANCOM switch), the two are auxiliary tags "SNMP device" and "LANCOM device" are set, because it has both properties.
In comparison, the tag "othersnmp" (other SNMP device" only sets the auxiliary tag "SNMP device", but not "LANCOM device".)
The top entry in this list is set as the default value. If you want to change the order of these values, you can use the arrow keys to move the entries. To delete a value, click on the waste bin .

4. When you have set all of the values for the tag, store your entries with "Save".

The list of tags is displayed again, and the new tag appears at the end of the list.



How to edit or delete a device tag or auxiliary tag

1. Select the entry "Device Tags" in the "CONFIG – Configuration" snap-in on the side bar on the main page.

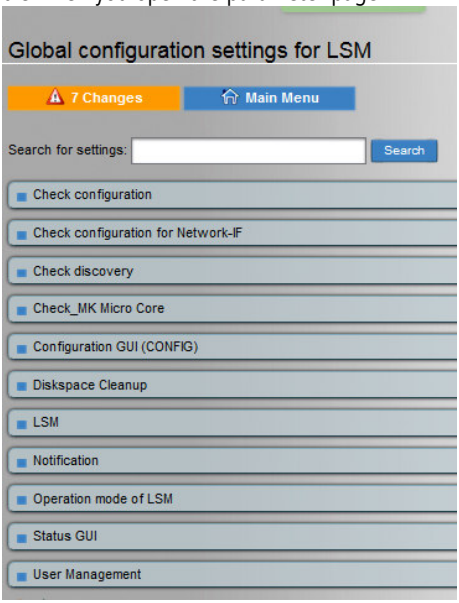
   An overview of the existing tags (device tags and auxiliary tags) opens up.
   You have several options:

   - With the help of the arrows  you can set the order of the individual tag rules.
   - Delete a tag with  .
   - To add new values, delete existing ones or change the default value, open the Details with  and proceed as described in step "3". Enter the parameters required for a device tag.

2. When you have completed your editing, store your entries with "Save".

5.8 Global settings

The Large Scale Monitor can be set up with one or more general configurations. These present a range of parameters in a clearly structured way (ON/OFF, or value). More information about each parameter is available when you open the parameter page.



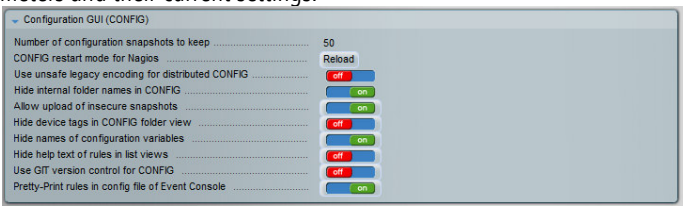
Various sections are available:

- Check discovery
- Configuring checks for network interfaces
- Configuring checks
- Diskspace cleanup
- Notifications
- User administration
- Operating mode of LSM
- Configuration GUI (CONFIG)
- LSM
- LSM status GUI

If you open a section of the general settings, you will see further information about each individual entry.

How to modify the individual parameters

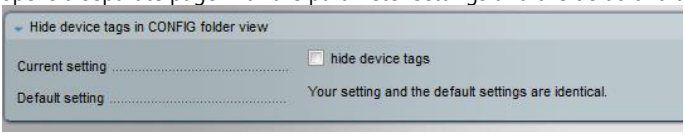
1. Open a range (here: Configuration (CONFIG)). Here you see an overview of the parameters and their current settings.



   Move the mouse over the parameter to display an explanation for it.

2. Click on one of the parameters (here: Hide the device tags in the folder view).

   This opens a separate page with the parameter settings and the default value.

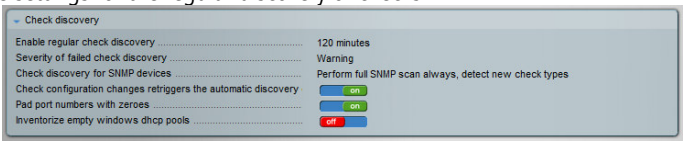


3. Click on  on the title bar for more information about the parameter settings.

4. Here, you can enable the option or specify new values.
5. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

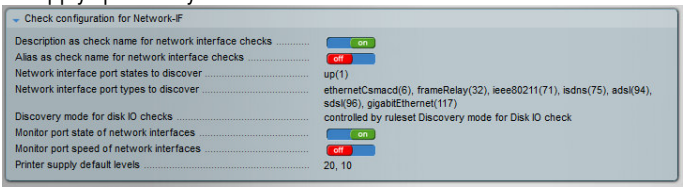
5.8.1 Check discovery

These are the settings for the regular discovery of checks.



5.8.2 Configuring checks for network interfaces

The checks that apply specifically to the network interfaces can be set here.

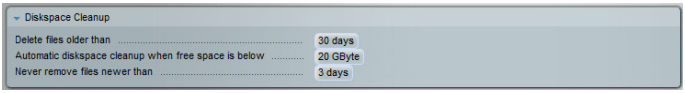


5.8.3 Configuring checks

This section explains the general configuration of the checks, for example log watch or toner status.

5.8.4 Diskspace cleanup

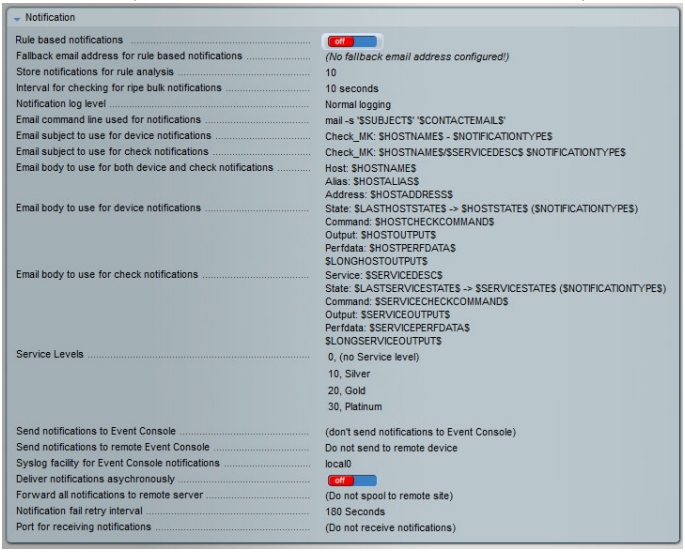
This allows you to determine which files are to be deleted if the available memory falls below a threshold.



5.8.5 Notifications

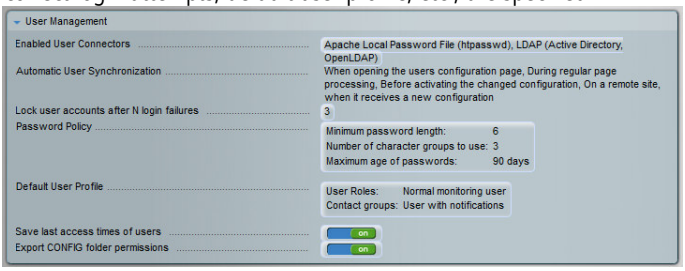
The content of notifications sent by the Large Scale Monitor is specified here, i.e. the subject line and the body of the message. There is a distinction between the different types of event (e.g. devices alert, check notification).

If rule-based notifications are disabled here (see section 5.15 "Rule-based notifications"), then user-specific notifications (see section 5.12.2 "User-defined notifications") can be configured.



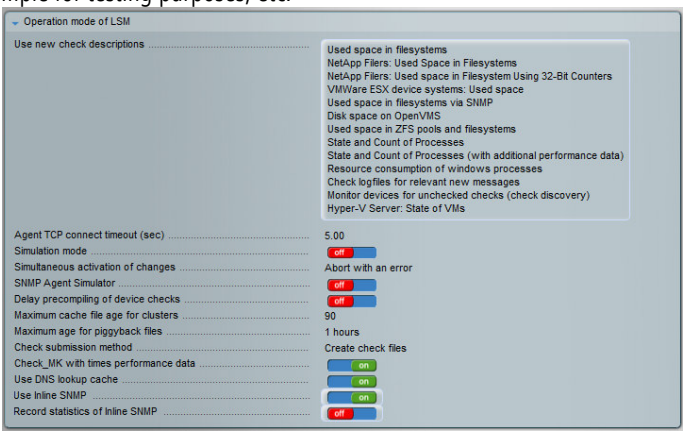
5.8.1 User administration

This is where the general user management settings, such as password management, the number of incorrect login attempts, default user profile, etc., are specified.



5.8.2 Operating mode of LSM

Settings concerning the current operation mode of the Large Scale Monitor can be adjusted here, for example for testing purposes, etc.



5.8.3 Check_MK Micro Core

The settings for the Check_MK Micro Core are adjusted here, such as the logging, time setting, and imports from the Nagios core.

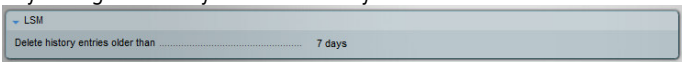
For details on how to change the core, see section 4.5 "Changing the monitoring core".

5.8.4 Configuration GUI (CONFIG)

The general behavior of the LSM configuration is determined here, e.g. the maximum number of saved snapshots, the uploading of snapshots, and the hiding of device tags or text.

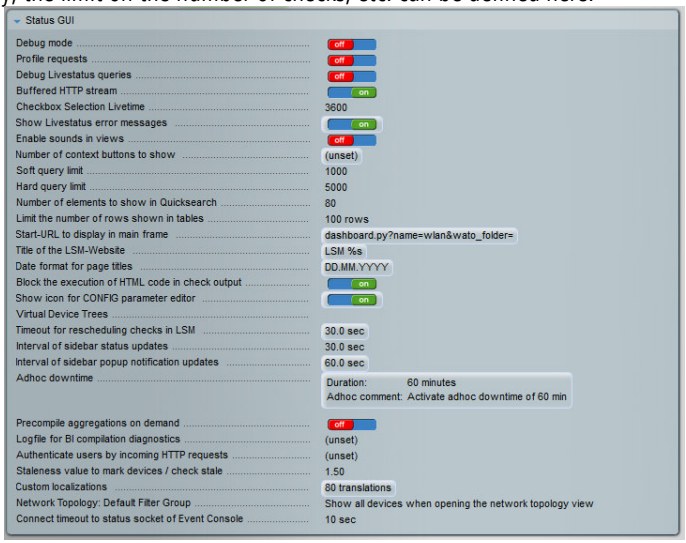
5.8.5 LSM

Here you specify the age of history entries that may be deleted.



5.8.6 LSM status GUI

The general setup of the LSM's interface, such as the debug mode, the internal suppression of folder display, the limit on the number of checks, etc. can be defined here.



5.9 Device & check parameters (rules)

This item displays the rules used by the Large Scale Monitor. The monitoring and also the grouping of devices are controlled by rules. The pre-configured rule sets are as follows.

- Active checks
  Checks relating to the network can be configured here.
- Grouping
  The assignment of checks and devices to groups is specified here.
- Monitoring configuration
  This item is for the general configuration of the monitoring, including the time periods and intervals, and the configuration of checks that do not appear in the automatic discovery.
- Access to agents
  This item is used to define the rules that control the communication of the monitoring with the SNMP agents and the Check_MK agents.
- Parameters for checks
  The rules for the parameters of the checks found by discovery are adjusted here.
- Datasource programs
  Rules for agents that provide access to further data sources, e.g. checks via SSH, SAP R/3, etc.
- Hardware/software inventory
  The hardware and software inventories are configured here.
- Event console
  Configuration and settings for the event console.
- Used rule sets
  Rules that are created will be assigned to one of the pre-configured rule sets. All of the rule sets displayed here contain at least one rule.

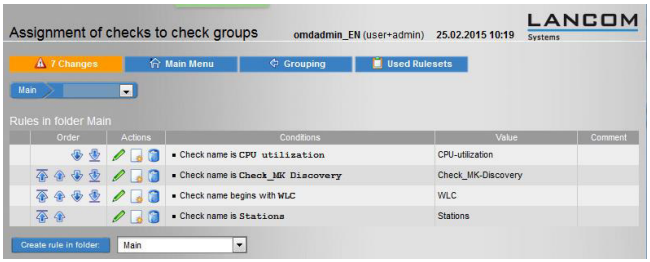
The order of the rules

The rules are executed in a specific order. The rules that were created in a subfolder are applied first, followed by the rules from a parent folder. Within a folder you can determine the order of application. To do this, open a rule (see below).

How to create or edit a rule

1. Select "Devices/check parameters" in snap-in "CONFIG – Configuration" in the side bar on the main screen.

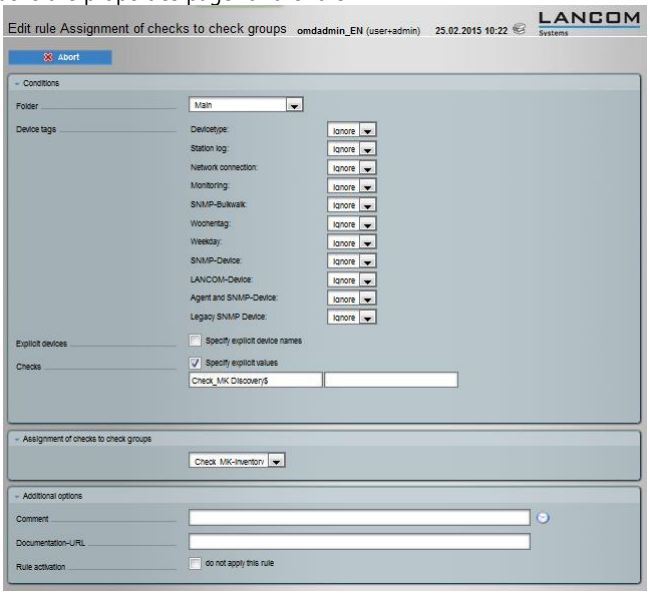
   An overview of the pre-configured rule sets opens up.
2. Click on the rule set that the new rule should belong to (e.g. Grouping).
3. This opens an overview of the pre-configured rule sets that control the way groups are treated, e.g. user groups, device groups or check groups. Also displayed is the number of rules in each group, and whether those rules were set in the current folder or imported from a parent folder.
4. Click on one of these groups (here: Assignment of checks to check groups).
5. The available rules are displayed.



Here you can

- edit an existing rule with  .
- delete an existing rule with  .
- change the order of the rules with  .
- create a new rule by copying an existing rule with  .
- The copied rule is placed in front of all the other rules. You can now edit this rule according to your needs with  .

6. This opens the properties page for the rule:



7. Here you set which mechanism the rule uses to assign the individual checks to the check groups:

- Conditions
  - Folders

    Set the folder that this check belongs to.
  - Device tags

    Specify if, when, and which attributes (tags) should be used for this check. In addition you can specify or exclude a particular device.
  - Explicit devices

    Here you can include or exclude devices by name. Regular expressions cannot be used here.
  - Checks

    You can additionally specify parts of the name that should receive this check. Entries made here are regular expressions that check for an agreement. A $ requires an exact agreement, a * stands for any string. Please note that with Windows systems the backslash (\) is dealt with separately and needs to be entered as \\. For example: "C:\\tmp\\message.log"
- Assignment of checks to check groups

  Select a check group that the check belongs to (here: CPU utilization).
- Additional options
  - Comment

    An optional comment explaining this rule.
  - Documentation URL

    An optional URL linking to documentation or another website. The link is displayed as an icon and opens a new page in the web browser. You can use either absolute URLs beginning with http:// or relative URLs beginning with /.
  - Rule activation

    The rule created in this way can be disabled.

8. If you have configured all of the parameters, you can backup your settings with "Save" or abort the action.
9. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

5.9.1 Example (setting the SNMP community with the help of a rule)

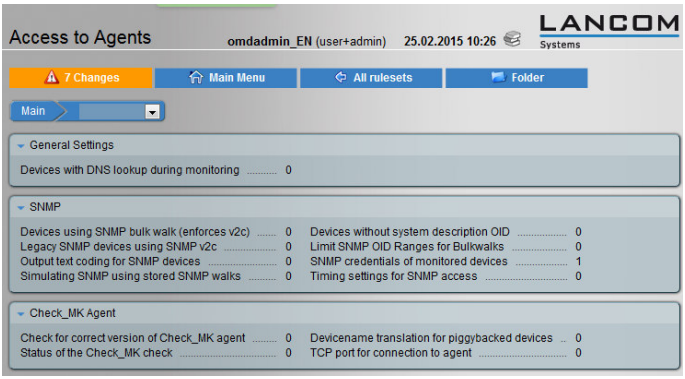
The SNMP community can also be set as a device property (see section 5.5.3 "Editing devices"). Here it serves as an example for a rule.

As an example of a rule set, the following describes how to set the SNMP community by means of a rule. The default community is "public". If this parameter is to be changed for certain devices, one or more rules can be created for it.

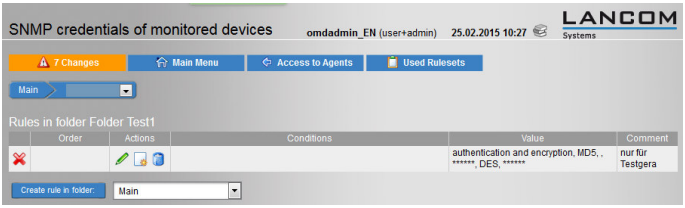
How to modify the SNMP community

1. Under CONFIG, select the menu item "Device & check parameters".

2. Select the "Access to agents" group.

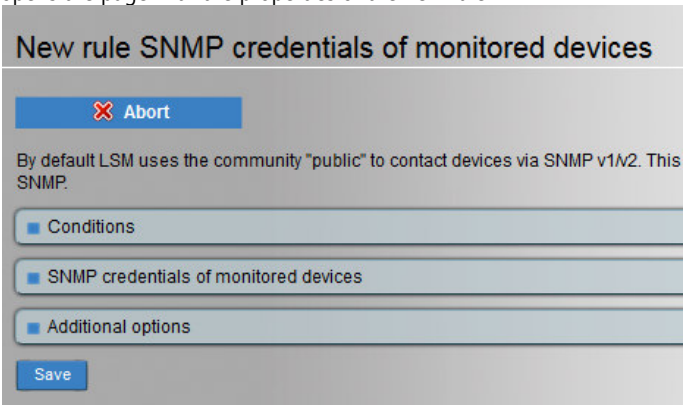


3. In the "SNMP" area select the "SNMP credentials for monitored devices" rule.

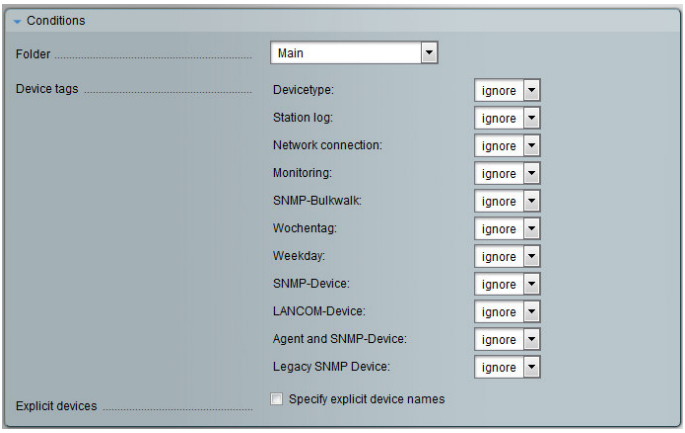


4. Click on "Create rule in folder". This sets whether the rule applies for all directories (usually "Main directory") or for a specific folder and its subfolders only.

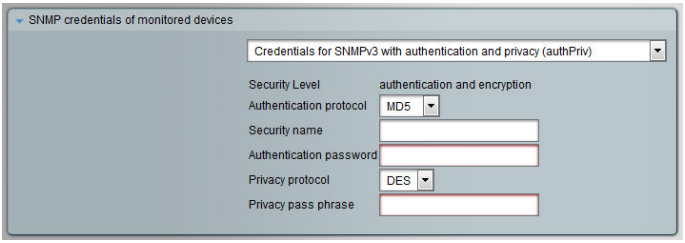
   This opens the page with the properties of the new rule:.



5. Under "Conditions" specify the devices for which you wish to change the SNMP community. It is also possible to set additional conditions that apply for this rule, such as the device type or even specific device names.

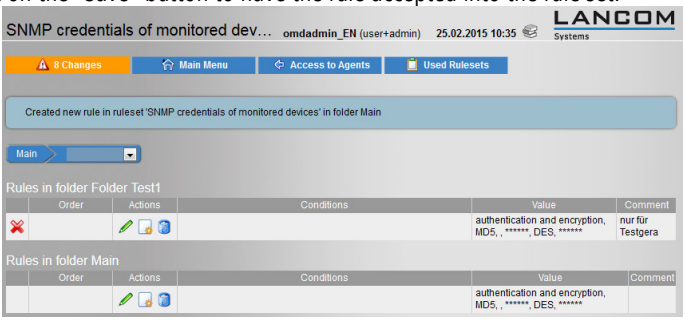


6. You can specify the SNMP community in the "SNMP credentials of monitored devices" section.



7. You can still add a comment and disable the rule under "Additional Options".

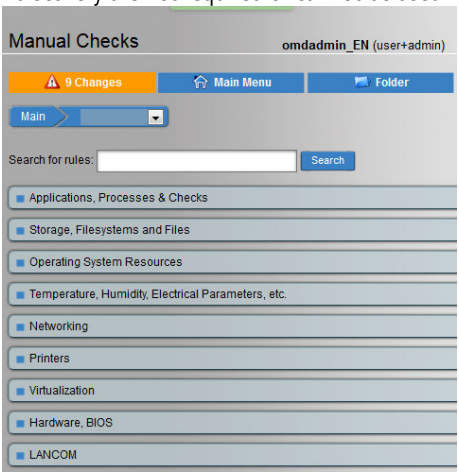
8. Click on the "Save" button to have the rule accepted into the rule set.



The rule is applied as soon as you enable the changes. Please refer to the section 5.4.2 "Activating changes" for more information about this.

5.10 Manual checks

You can manually create rule sets for checks here. This is useful if the checks assigned automatically by the bulk discovery are not required or cannot be used.



You can create a new set of rules from the variety of existing rules. How you create rules is explained in the section "How to create or edit a ruleHow to edit the rules that assign the devices to the device groups".

5.11 Device & check groups

Devices can be organized into groups. This configuration is an orthogonal complement to the folder structure in that it provides access to similar devices. For example, it allows all PCs within the network to be grouped together. Thus if the device "PC" is addressed, all PCs in the network will be addressed regardless of which folder they are located in.

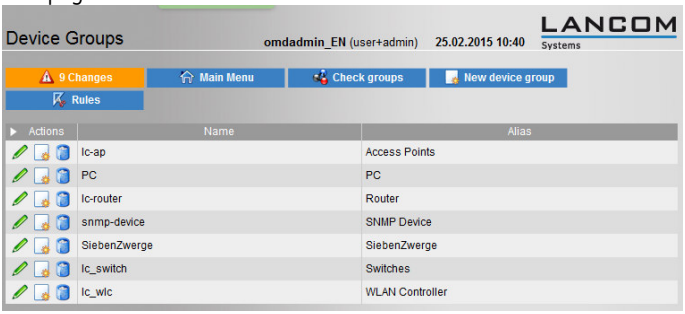
Some groups are set during installation:

- PC - Computers within the network
- lc-ap - LANCOM access points
- lc-router - LANCOM routers
- lc_switch - LANCOM switches
- lc_wlc - LANCOM WLAN Controller
- snmp-device - Any device with SNMP

The pre-configured device groups can be edited with or deleted with .

How to create, edit or delete a device group

1. Select "Device & check groups" in snap-in "CONFIG – Configuration" in the side bar on the main page.



An overview of the pre-configured device groups opens up.

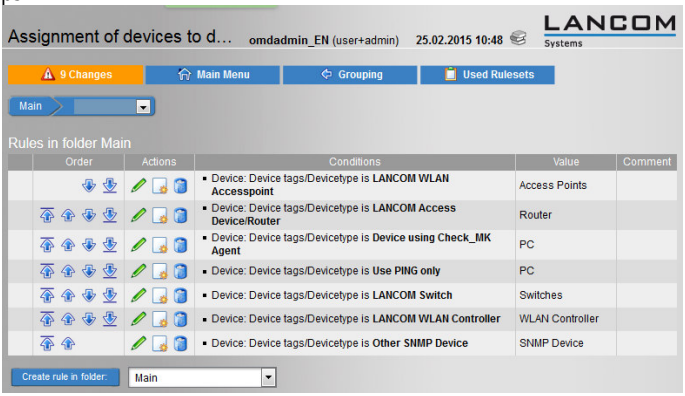
2. The pre-configured device groups can be changed , copied or deleted here. Create a new group with "New device group".

This opens the page for defining a new group:

3. Given a name and an alias for the new device group and confirm your entry with "Save".
4. You can change the parameter "Alias" subsequently, but not the name of the device group.
5. The new device group is now ready for further configuration.

How to edit the rules that assign the devices to the device groups

1. Select "Device & check groups" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. An overview of the pre-configured device groups opens up.
3. The "Rules" button opens a list of rules which assign the individual devices to the device groups.



4. Here you can
   - edit an existing rule
   - delete an existing rule
   - change the order of the rules
   - Create a new rule by copying an existing rule .
   - The copied rule is placed in front of all the other rules. You can now edit this rule according to your needs .
5. Use the selection list "Create rule in folder" to determine which folder the rule is to be created in. For more information please refer to section "How to create or edit a rule".
6. The changes are immediately entered into the list of changes.
7. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

5.11.1 Check groups

Checks are also grouped. This configuration is an orthogonal complement to the folder structure in that it provides access to checks that are similar to one another. For example, it allows all of the checks relating to CPU utilization in the network to be grouped together. If the Check group "CPU utilization" is selected, then all these checks are activated irrespective of the folder they are located in.

The default installation already contains some predefined Check groups:

- CPU utilization — All checks relating to CPU utilization.
- Check_MK-inventory — All checks that are named "check_MK-inventory".
- Stations — All checks that are named "Stations".
- WLC — All checks with a name beginning with "WLC"

The pre-configured check groups can be changed  , copied  or deleted  here. The procedure is analog to the creation of device groups.

5.12 User

During installation, an “omdadmin” user is created for the administration of the Large Scale Monitor (password: "omd") (see chapter 4.2 "Running the installation").

Create further new users in order to be able to

- set up the distribution of notifications to different users
- assign specific roles to individual users
- restrict the rights of individual users
- assign personal views to users.

User attributes

With this button you can specify further individual user attributes, such as their department or workplace.

How to create a new user

1. Select "User" in the "CONFIG – Configuration" snap-in on the side bar on the main page.

   An overview of the existing users is displayed.

2. Here you can

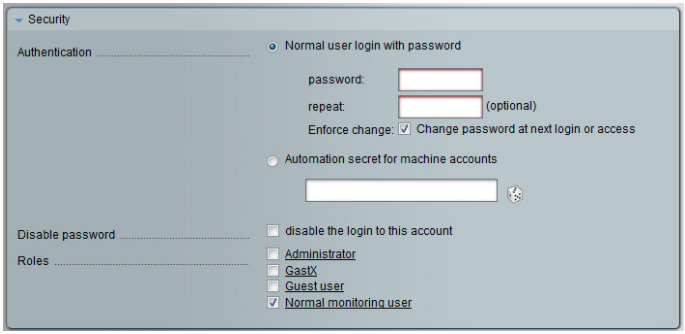
   - edit an existing user
   - delete an existing user
   - create a new user by copying an existing one. This immediately opens a dialog box with the user properties and you must enter a new user name and a corresponding password.
   - Click “New User” to create a new user.

3. This opens a dialog box with the user properties.

Identity

Enter the user name here, the person's full name or more detailed information, their e-mail address, if they are to receive messages and, where available, the user's pager address.
The user name is compulsory, it must be unique and cannot subsequently be altered.

Security



Define the method of authentication:

- Authentication:

  Enter the password here and confirm it. Make sure that the password contains characters from three different groups of characters (A-Z, a-z, 0-9 and special characters).
  Here you can the user to change the password at the next login.

- Automation secret for machine accounts

  This setting is used to communicate between other programs and the Large Scale Monitor. This is required only if the configuration of another program requires it. Click on the dice  and the system will generate a security code. The authentication information stored in a local file can then be used by the program for automated processing. To this end, the program must at least have read access to this file.

- Disable password

  The configured user is no longer able to log in.

- Roles

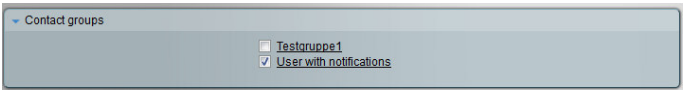
  Define the new user's roles
  (see section 5.12.1 "Restricting users"). A role must be assigned to the user.

- Sites

  Specify whether this user is known at all sites or at specific sites only, i.e. he/she can login there only (see section 5.18 "LSM connections").

Contact groups

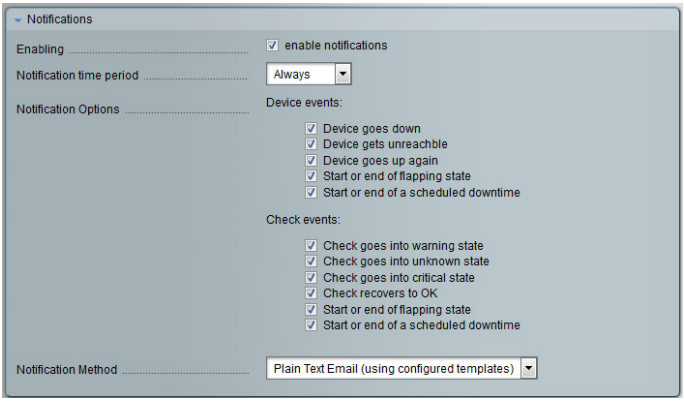
In Contact groups you define whether users can view devices during monitoring or whether they receive notifications from the devices. The notifications are always sent to a Contact group. During installation just one group is installed, "User with notifications".



If a user is to receive notifications, select at least one Contact group that the user is to be a member of.

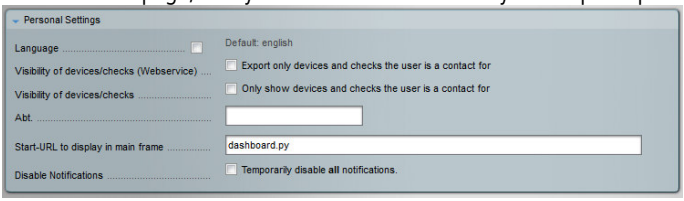
Notifications

You can define here if this user is to receive notifications and, if so, during which time period and what types of notifications. An e-mail address must be specified If notifications are to be sent to a user. Please refer to section 5.12.2 "User-defined notifications" for further information.
Requirement: Rule-based notifications are disabled in the LSM's global settings (see section 5.8.5 "Notifications"). User-specific notifications cannot be configured here if rule-based notifications are enabled.



Personal settings

You can set the language of the user interface here (German/English, default: English), the personal home page, and you can restrict the visibility and export options.



4. Once you have configured all the parameters, click “Save” to store your settings.
5. An overview of all configured users is displayed.
6. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

5.12.1 Restricting users

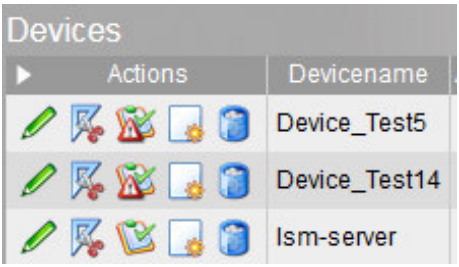
A differentiation must be made here between configuration restrictions and monitoring restrictions. These restrictions basically apply only to users without administrative rights. Administrators are not subject to any restrictions.

For normal users to be able to configure folders or devices they must be granted the appropriate rights. These rights can be granted to them via the folder or device properties. As rights can only be assigned to a group, you must ensure that the selected user is member of a contact group. In addition, you should assign configuration or monitoring rights to this group for the device or folder.

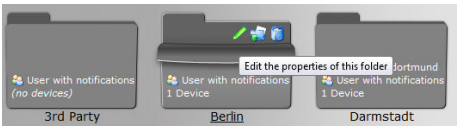
How to assign configuration rights to a user for a folder / device

1. Assign the user to a group (see section „5.14Contact groups").
2. Select "Devices & Folders" in the "CONFIG – Configuration" snap-in on the side bar on the main screen and then select the corresponding folder.
3. An overview of the available devices or folders is displayed.

   - Devices



   - Folders

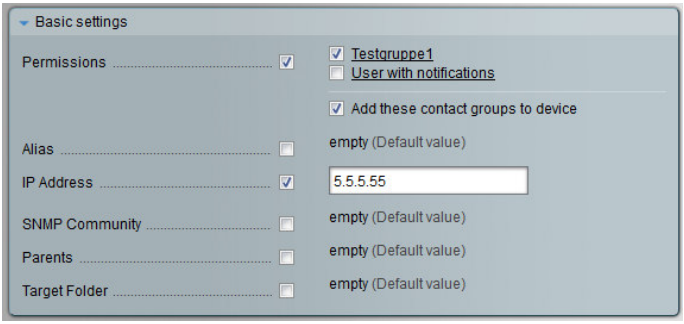


4. Select the Edit properties icon.

   This opens "Basic Settings" in the properties dialog box.

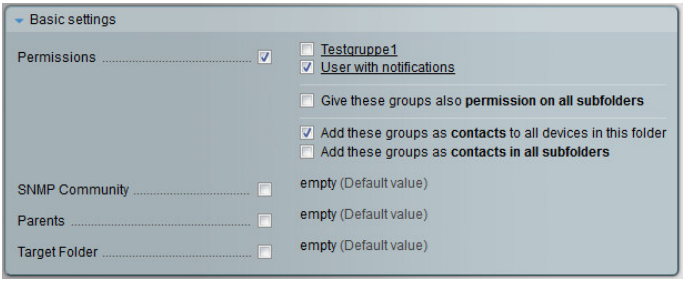
5. Select the "Permissions" check box. A list of the currently configured groups is displayed.

   - Devices



     Select the checkbox for the group of which the user is a member. This assigns configuration rights to the user.

- Folders



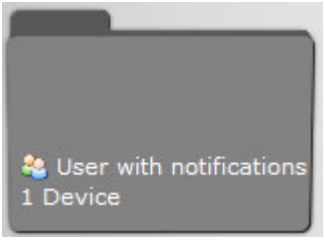
- Configuration rights

  Select the check box for the group that the user is a member of. This assigns configuration rights to the user for this folder.
  Where the user is also to be allowed to configure the subfolders, enable "Permission for subfolders".

- Monitoring rights

  If the user is to be allowed to view the folder during monitoring, add the group to the "Contacts" for all devices.
  Where the user is also to be allowed to monitor the devices in the subfolder, add the group to the "contacts in all subfolders".
  The monitoring right can only be assigned in conjunction with the configuration right, it cannot be assigned separately.

6. Once you have configured all the rights, click “Save & Finish” to save your settings.
7. The groups with the configuration rights to this folder are then displayed on the folder itself.



5.12.2 User-defined notifications

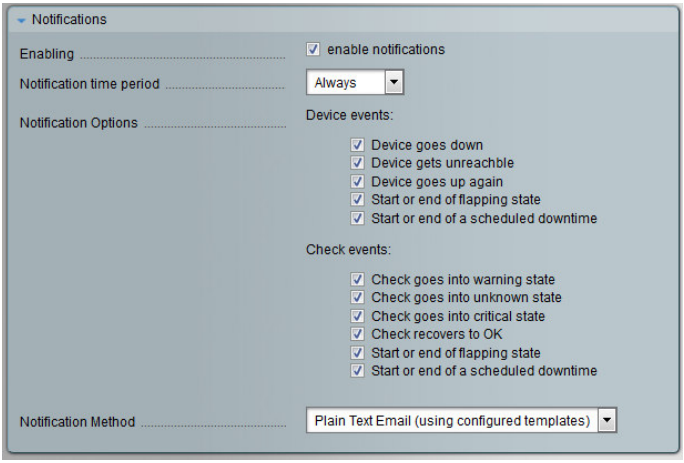
Each user can be sent specific notifications. For example, these can refer only to specific devices or checks, or only be sent during specific time periods or in specific escalation stages.

➢ NOTE: If all user-defined notifications have been individually disabled no notifications will be sent, even though they appear to be enabled in the "Notifications" area (check box). There is no fall back to the default notification.

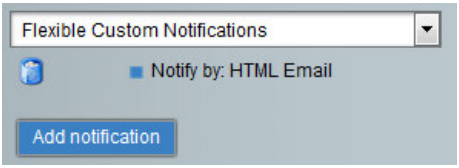
How to configure user-specific notifications

Requirement: Rule-based notifications are disabled in the LSM's global settings (see section 5.8.5 "Notifications"). User-specific notifications cannot be configured if rule-based notifications are enabled.

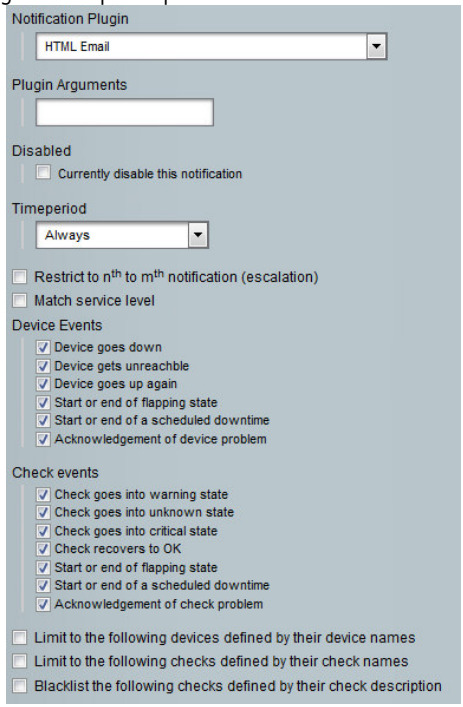
1. Select "User" in the "CONFIG – Configuration" snap-in on the side bar on the main page.
2. An overview of the existing users is displayed.
3. Open a user's properties or configure the user-defined notifications directly when you create a user profile.
4. In order for the Nagios system to send the database for the notifications to the LSM, ensure that the notification is enabled in the "Notifications" section
   - in the user profile (check box),
   - the time period "Always" is selected and
   - all device and check events have been selected.



5. Select "User-defined notification" as "Notification Method".
6. Click on the "Add notification" button.



7. Click on the button "Notify by: HTML e-mail".
   The e-mail configuration opens up.



- Notification plugin

  Select here the way in which the notification is to be sent. Bear in mind that the contact details for e-mail and SMS notifications must be specified in the "Identity" area (default: HTML e-mail).

- Plugin Arguments

  Currently on the parameter "Send an SNMP TRAP to Receiver (1) with community (2)" is required, with the recipient in the first field and the community in the second.

- Deactivated

  Here the currently defined notifications can be disabled.

- Time period

  Here the time period can be selected (default: Always). For details on how to set new time periods see section 5.16 "Time periods".

- Restrict to nth to mth notification (escalation)

  The range of escalations can be restricted here, e.g. as of the 10th one.

- Match service level

  Where service levels have been specified, notifications can be set for specific service level areas only.

- Device and check events

  Specify the events for which a notification is required (default: All).

- Limitations

  Notifications can be limited to specific devices and checks listed here by name. Pay attention to the used of upper/lower case in device names. Use ! for negation and ~ for regular expressions.

- Blacklisted checks

  Checks can be excluded based on their description. If you use regular expressions, the start of the check description must agree.

8. Click again on "Add notification" if you would like to configure further notifications.
9. If several user-defined notifications have been specified, you can change the sequence with the arrows  .
10. Notifications that are no longer required can be deleted with  .
11. Close the configuration with "Save".

5.12.3 Spontaneous notification

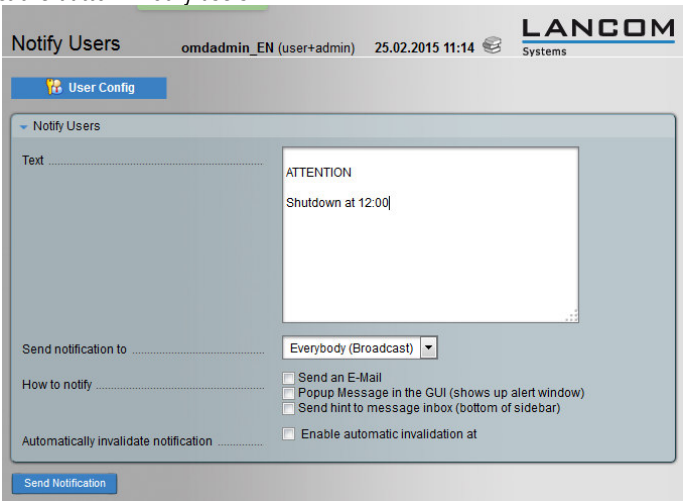
All (logged-in) users can be sent a spontaneous notification, for example for maintenance purposes.

How to send a spontaneous notification

1. Select "User" in the "CONFIG – Configuration" snap-in on the side bar on the main page.

   An overview of the existing users is displayed.

2. Select the button "Notify users".



3. Write the message in the text field.
4. The recipient can be specified in more detail:
   - Everybody (broadcast)
   - All active users
   - A specific list of users. These can be selected from a list.
5. Specify the type of notification:
   - Send e-mail.
   - Pop-up message in the GUI.
   - Display a note at the foot of the side bar.
6. You can define when the message is invalidated.
7. Click on the "Send Notification" button to send the message immediately.

5.13 Roles and permissions

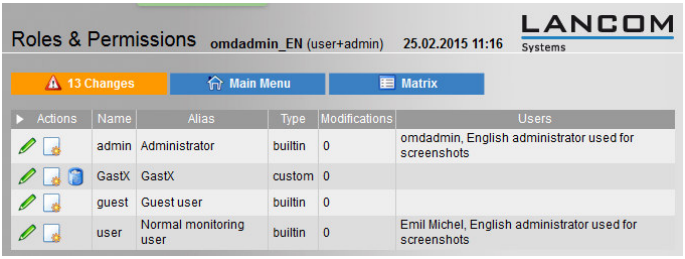
The rights to configure or monitor devices or folders are always assigned to groups. Set up the corresponding groups for this.

Please refer to section 5.14 "Contact groups" for further information.

How to create a new role or edit an existing role

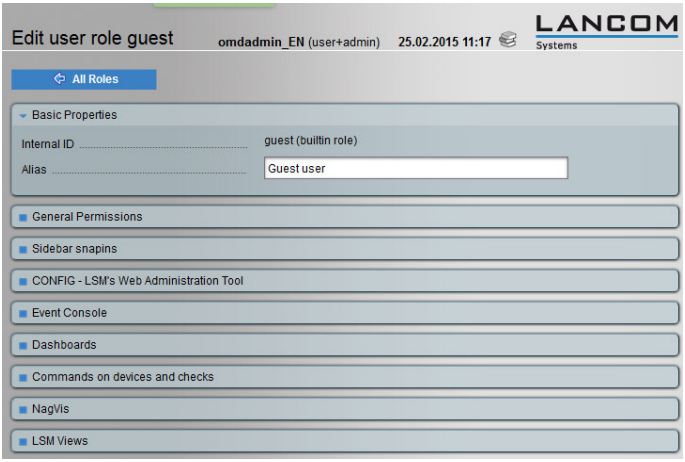
1. Select "Roles & Permissions" in the "CONFIG – Configuration" snap-in in the side bar on the main page.
2. An overview of the available roles is displayed.

   The "admin", "guest" and "user" roles are default roles and cannot be deleted.



3. Here you can

   - edit an existing role
   - delete an existing role as long as it not a default role
   - create a new role by copying an existing role A user role is then added to the list, and an "x" is added to the name. You can now edit this role .



4. Configure the role properties:

   - Default properties

   Define the internal ID here. This cannot be altered subsequently. Assign a descriptive alias that is preferably different from the current alias. This will appear later in the interface as the name of the role. Select the template for the new role from the drop down list. Assign the individual permissions here. The default setting, based on the role template, can be enabled or disabled in the drop down menu.

   - General permissions
   - Web API
   - Side bar snap-ins
   - CONFIG – LSM's web administration tool
   - Event console
   - Dashboards
   - Commands for devices and checks
   - NagVis
   - Views

   The online help  in the title bar offers you further information on every setting.

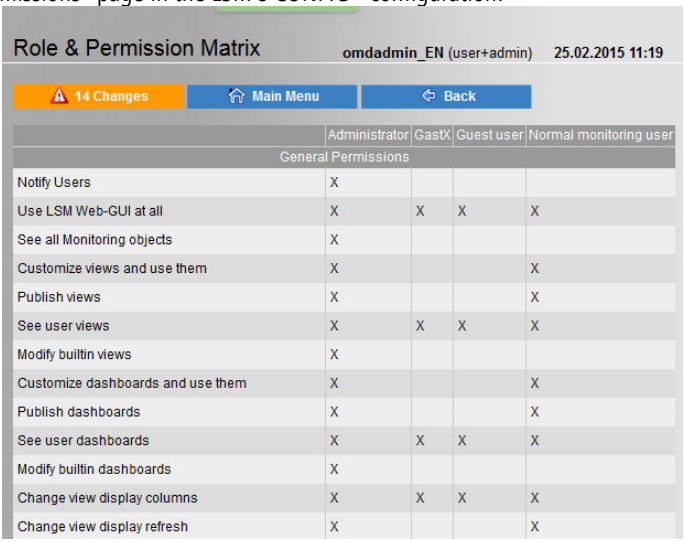
5. Once you have configured all of the permissions, click "Save" to store your settings.

   An overview of all roles is displayed. Changes are included in the change list.

6. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

Matrix

All permissions can also be set out in a matrix. To do this, click on the "Matrix" button to the "Roles & Permissions" page in the LSM's CONFIG - configuration.



Role & Permission Matrix

omdadmin_EN (user+admin) 25.02.2015 11:19

14 Changes | Main Menu | Back

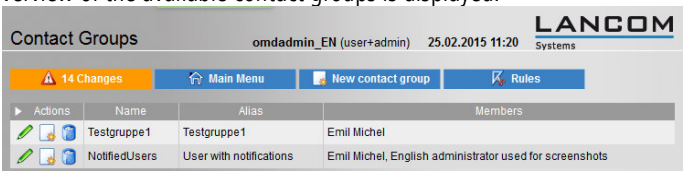
	Administrator	GastX	Guest user	Normal monitoring user
General Permissions				
Notify Users	X			
Use LSM Web-GUI at all	X	X	X	X
See all Monitoring objects	X			
Customize views and use them	X			X
Publish views	X			X
See user views	X	X	X	X
Modify builtin views	X			
Customize dashboards and use them	X			X
Publish dashboards	X			X
See user dashboards	X	X	X	X
Modify builtin dashboards	X			
Change view display columns	X	X	X	X
Change view display refresh	X			X

5.14 Contact groups

Contact groups are used to set notifications for particular users and to assign configuration or monitoring rights.

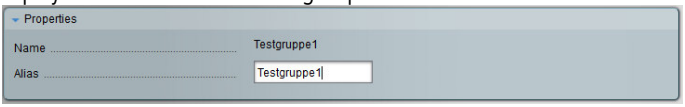
How to create a new group or edit an existing group

1. Select "Contact groups" in the "CONFIG – Configuration" snap-in on the side bar on the main page.
2. An overview of the available contact groups is displayed.

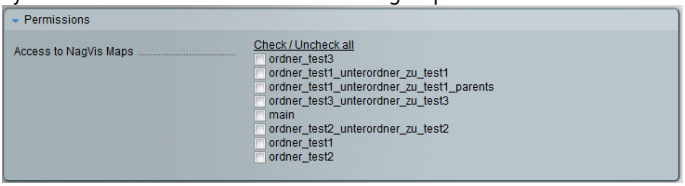


3. Here you can

   - edit an existing contact group
   - delete an existing group
   - create a new contact group with "New contact group".
   - display the rules for the contact group "Rules".



4. Assign a name and an alias. The name cannot be altered subsequently. The alias is displayed in the interface as the name of the group.



5. Specify the folder where the contact group configured here receives access the stored maps.
6. Once you have configured your group, click “Save” to store your settings.

   An overview of all contact groups is displayed. Changes are included in the change list.
7. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

For details on how to add a user to this group see section 5.12 "User".

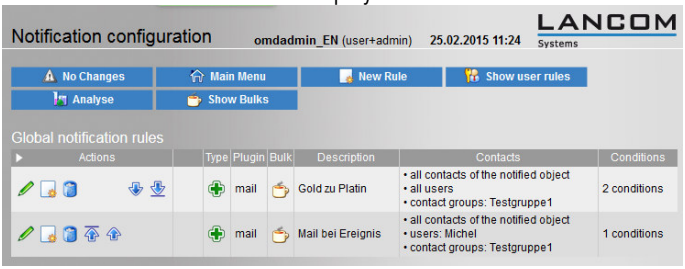
5.15 Rule-based notifications

Notifications can be set to users, contact groups, or other addresses by e-mail, SMS or system message if certain conditions are met. These notifications are specified by rules. Several rules are listed in a priority list in which the rules are tested in sequence.

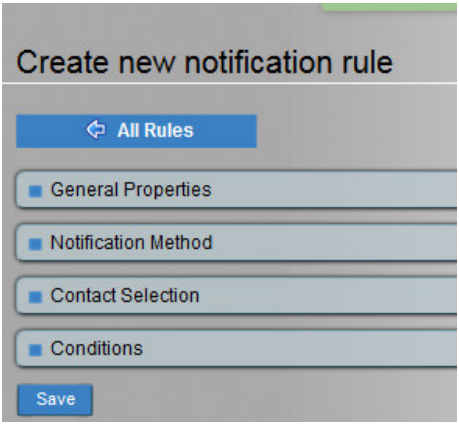
➢ NOTE: Rule-based notifications need to be enabled in the LSM's global settings (see section 5.8.5 "Notifications").

Creating a new rule

1. Select "Notifications" in the "CONFIG – Configuration" snap-in on the side bar on the main page.
2. An overview of the available rules is displayed.

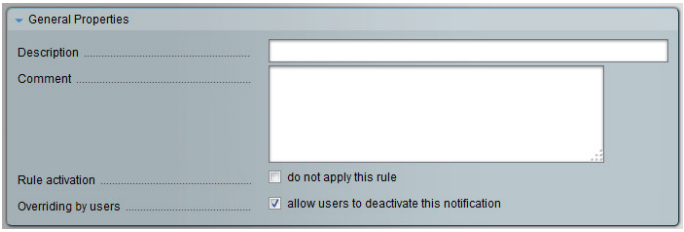


3. Select "New Rule"



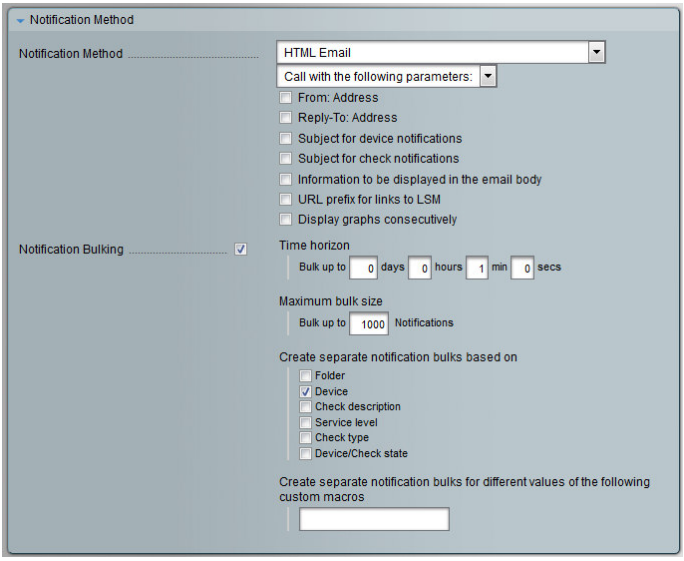
4. Create the properties for this rule:

General properties



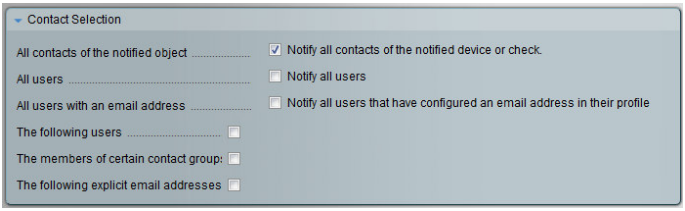
Select a meaningful description here. You can disable the rule and allow those users affected by it to disable it from their side.

Notification method



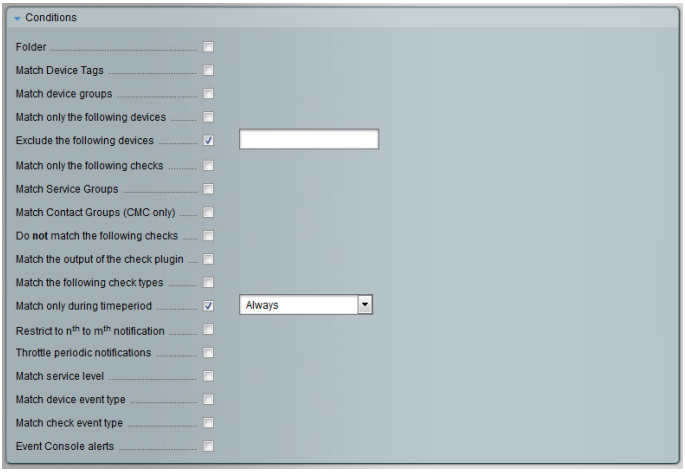
Select here how the user is to be notified. You can choose between different e-mail formats, SMS, or system messages. Set the format of the e-mail (sender, subject and content).
You also set the time horizon, the maximum size, and the separation of bulk messages for different elements.

Contact selection



Here you can determine which users are notified. You can add additional e-mail addresses as well as those already in the system.

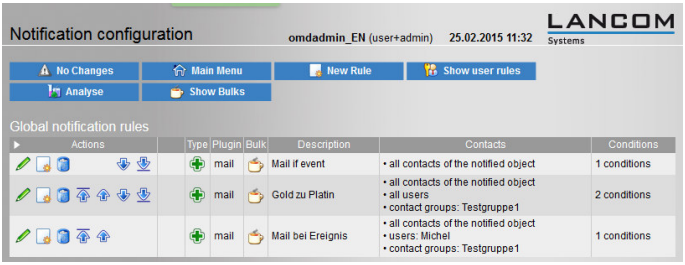
Conditions



Here you specify the conditions for sending a notification.

5. Click “Save” to save the rule.

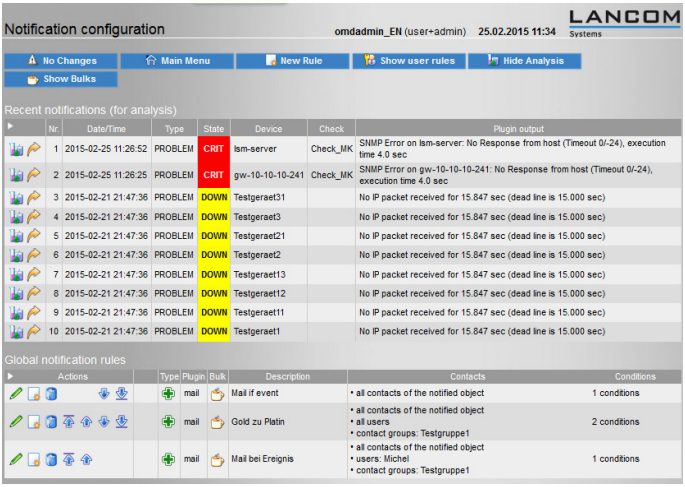
You see an overview of all global notification rules.



6. Here you can change the order of the rules with the arrows  . The rules are processed from the top down.

Analyzing notification rules

"Analyze" allows you to display previous notifications. Use  to resend a notification from the list of notifications.



If you click on Analyze  in the row of a notification, you will see if a rule applies to this notification (green) or not. The corresponding rule is also highlighted in green in the list of rules. Below it is a list of sent messages.

Bulk notifications

Bulk notifications refer to notifications to multiple recipients, but also multiple notifications that need to be sent.

You can hide bulk notifications with "Hide Bulk".

User-specific notification rules

The "Show user rules" button displays the notification rules created for individual users. For details on how to create these rules see section 5.12.2 "User-defined notifications".

5.16 Time periods

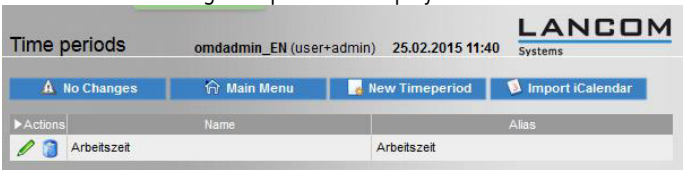
Time periods are defined to

- send notifications to different addressees (see section 5.14 "Contact groups")
- restrict monitoring to certain times (see "How to create a new time period")

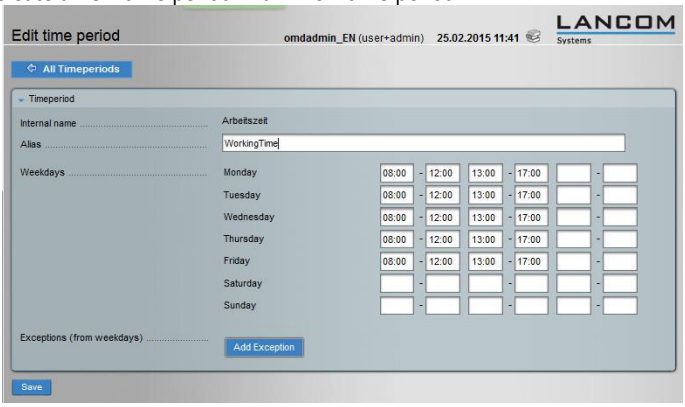
No time periods are defined in the default installation, although there is an internal time period, “Always”.

How to create a new time period

1. Select "Time periods" in the "CONFIG – Configuration" snap-in on the side bar on the main page.
2. An overview of the existing time periods is displayed.



3. Here you can
   - edit an existing time period
   - delete an existing time period
   - create a new time period with "New time period".



4. assign an internal name (the name “Always” cannot be used) which subsequently cannot be altered. The alias name should be indicative of the time period.
5. Define the time periods for each week day.
6. Where necessary define individual exceptions.
7. Exclude any time periods that have already been defined.

8. Once you have configured a time period, click "Save" to store your settings.
9. An overview of all time periods is displayed. Changes are included in the change list.
10. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

Importing an iCalendar file

You can import here the data from an *.ics file here. Click the "Import iCalendar" button

5.17 Log file content Analyzer

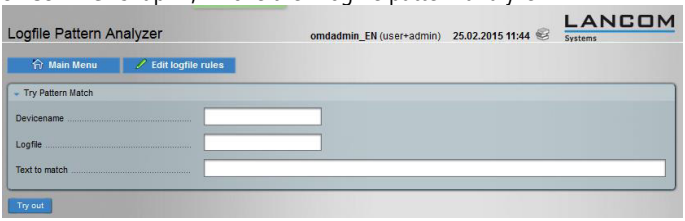
Windows and Linux devices create log files while they operate. If you select a device allows you can view all of the checks for this device. The log files are checked at the same time. You can identify the checks for these log files with the icon . Click on this icon to view the log file.

These log files can be further analyzed using the rule set. For example, statuses can be changed based on log file entries (e.g. from CRITICAL to IGNORE). The analyzer helps to examine this rule set.

Beforehand, at least one rule must be created for the log file. This can be specified using the rule editor. When you create it, a regular expression is created, which is referred to as a pattern.

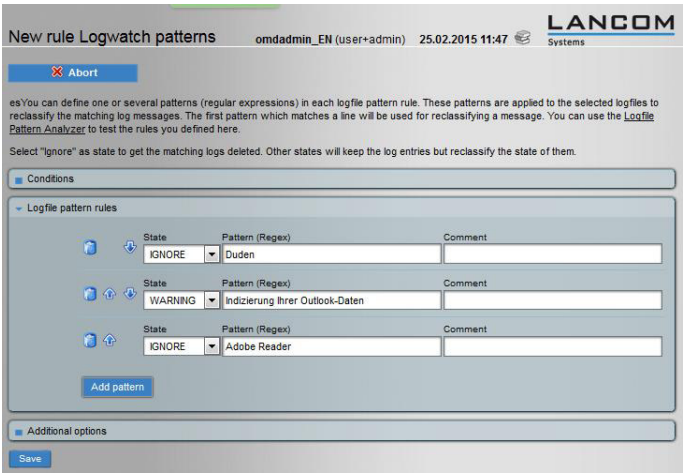
How to analyze the rule set for the log file content

1. In the "CONFIG" snap-in, invoke the "Logfile pattern analyzer".



2. Enter the name of the device that you want to analyze.
3. Use "Edit logfile rules" to change to the rule editor in order to create a rule for analyzing the log file.

4. Select the directory that the rule is to apply to and click on "Create rule in folder".



5. Define the rule here:

   - Conditions

     Here you can specify the devices (device tags, names) for which this rule is to apply.

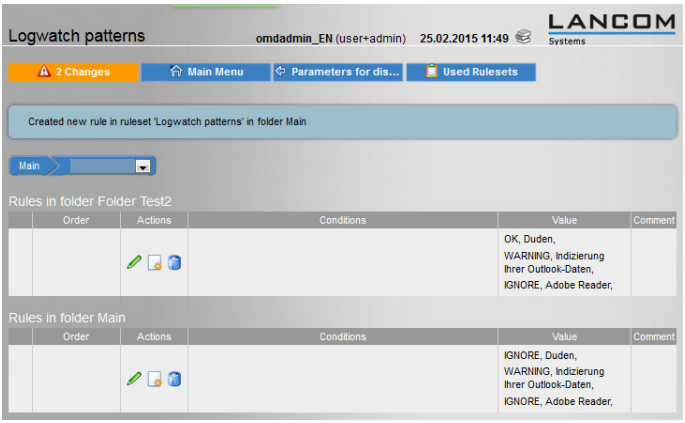
   - Rules for the log file pattern

     Here you specify which pattern is to lead to which state (example: All log messages containing the string "Duden" should lead to the "IGNORE" state.)
     If you have more than one pattern, set the order of the pattern analysis. A rule only checks until the first applicable pattern is found. All other later patterns are not considered.

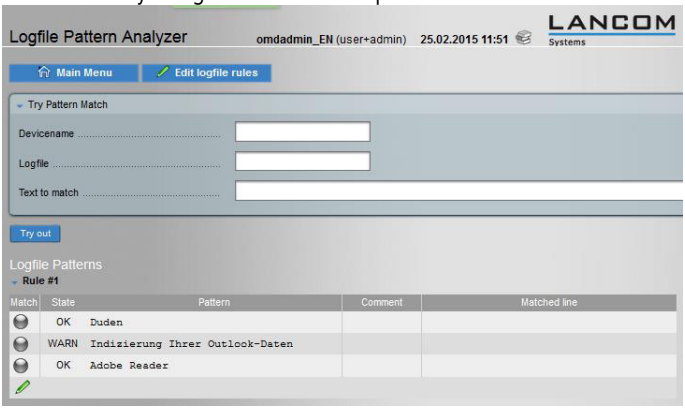
   - Additional options

     You can deactivate the rule here, or add further comments.

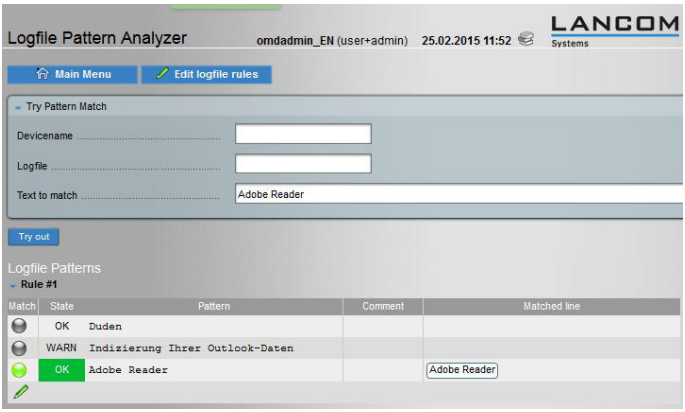
6. With "Save" you complete the rule creation and return to an overview of the log file patterns.



7. Now start the Analyzer again. The different patterns are now all listed.



8. Now you can enter a device, the log file, and text under "Try pattern match". "Try out" shows if a pattern matches the entered text.



A pattern match is highlighted in green with .

You can continue to edit the rule directly with .

9. If you are finished creating your rules, please activate the changes you have made.

5.18 LSM connections

The monitoring of multiple sites can be configured here. This function is currently not part of the product and will only be included in individual projects.

5.19 Backup & restore

Making a backup is recommended where changes have been made to the system after installation. A snapshot (backup) is automatically created at each startup. Any changes that have been made but not yet activated will also be stored when the snapshot is created.

System snapshot

A system snapshot saves the following data (default):

- Authentication
- Devices, checks, groups, time periods and monitoring settings
- The event console configuration

User-defined snapshot

You can initiate a snapshot yourself. In doing so you can specify what this snapshot saves (see "How to create a backup copy").

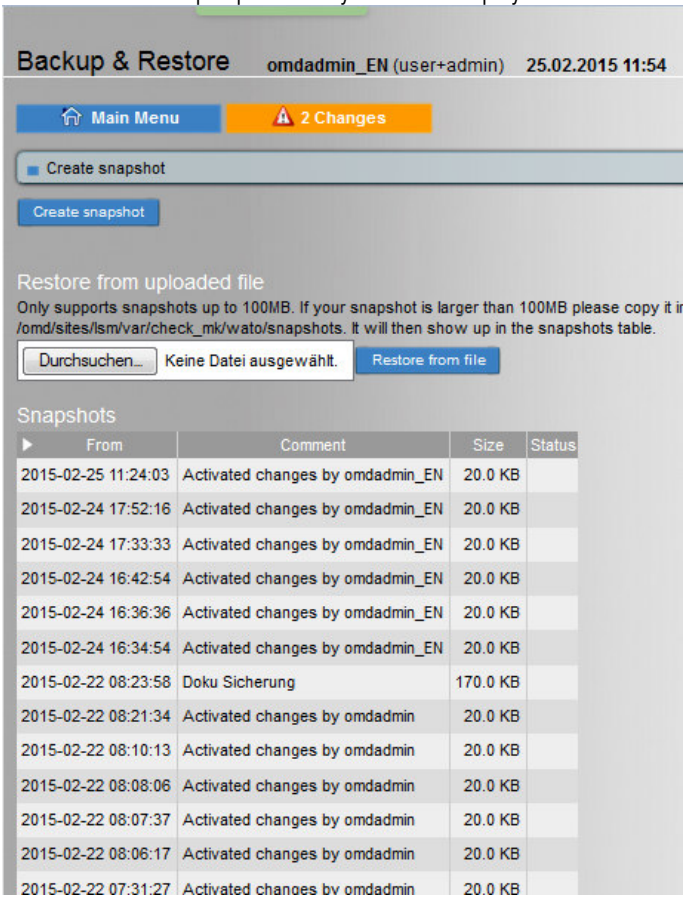
Restore

You can restore a backup copy at any time. Alternatively you can also delete all changes that have been made and restore the factory settings. The backup copies can also be saved locally and restored from this location (see How to restore a previous configuration).

➢ NOTE: The default backup (system snapshot) contains the configuration data for the Large Scale Monitor. Not included are logged data and maps with the device locations.

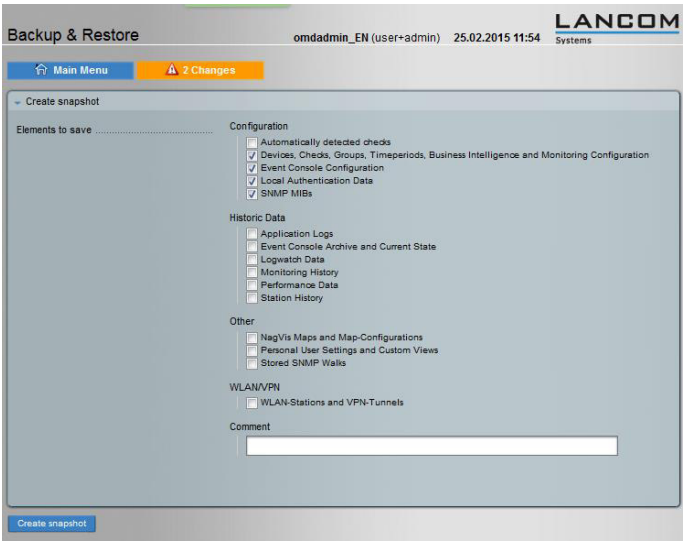
How to create a backup copy

1. Select "Backup & Restore" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. You can configure and start a snapshot directly in the upper field. Further down an overview of the all backup copies already created is displayed.



From	Comment	Size	Status
2015-02-25 11:24:03	Activated changes by omdadmin_EN	20.0 KB	
2015-02-24 17:52:16	Activated changes by omdadmin_EN	20.0 KB	
2015-02-24 17:33:33	Activated changes by omdadmin_EN	20.0 KB	
2015-02-24 16:42:54	Activated changes by omdadmin_EN	20.0 KB	
2015-02-24 16:36:36	Activated changes by omdadmin_EN	20.0 KB	
2015-02-24 16:34:54	Activated changes by omdadmin_EN	20.0 KB	
2015-02-22 08:23:58	Doku Sicherung	170.0 KB	
2015-02-22 08:21:34	Activated changes by omdadmin	20.0 KB	
2015-02-22 08:10:13	Activated changes by omdadmin	20.0 KB	
2015-02-22 08:08:06	Activated changes by omdadmin	20.0 KB	
2015-02-22 08:07:37	Activated changes by omdadmin	20.0 KB	
2015-02-22 08:06:17	Activated changes by omdadmin	20.0 KB	
2015-02-22 07:31:27	Activated changes by omdadmin	20.0 KB	

3. Open the "Create snapshot" section.



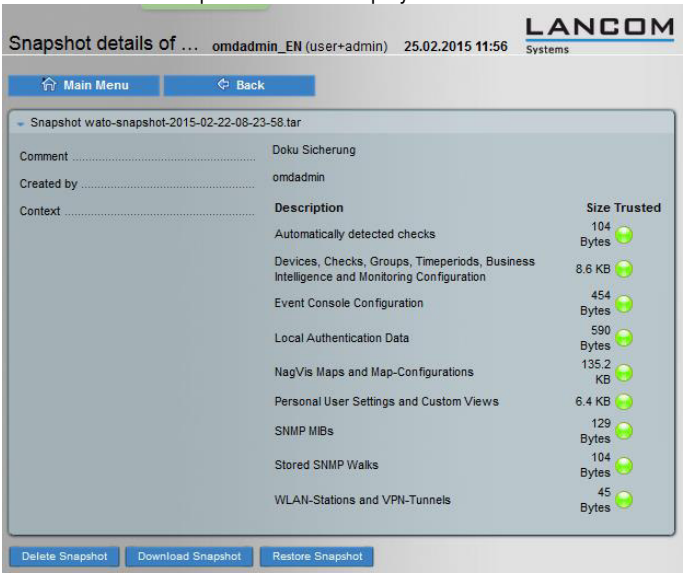
4. Specify which data needs to be backed up and enter a comment.
5. Click “Create snapshot”.

   A clock  in the snapshot list shows that the snapshot is being created.
   Reload the page (F5) to acknowledge completion as there is no automatic update.

► The snapshot settings are reset to the standard vale for the system snapshot.

How to externally save a backup copy

1. Open the list of backup copies in the "CONFIG – Configuration | Backup & Restore" menu.
2. Click directly on the name of the snapshot file you wish to backup.
3. An overview of the backup file details is displayed.



4. Download opens the local download manager for the web browser.
5. Specify the storage location, preferably local, and save the file.

How to restore a previous configuration

1. Select "Backup & Restore" in snap-in "CONFIG – Configuration" in the side bar on the main page.
2. An overview of the all backup copies already created is displayed.
3. You have several options:
   - Restore a snapshot that has been saved locally.

     Use the "Browse…" field and enter the path to this file. Select "Restore file" to begin the restore process.
   - Restore a snapshot from the list (saved to the system).

     To do this, click on the name of the snapshot. The details of this snapshot are displayed. Select "Restore Snapshot" to start the restore process.

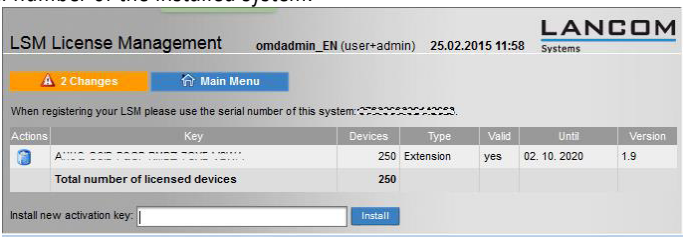
5.20 LSM License Management

Please enter an activation code soon after system installation.

➢ NOTE: Ensure that you retain the activation code that you received at time of purchase.

How to obtain an activation code

1. Select "LSM License Management" in the "CONFIG – Configuration" snap-in on the side bar on the main page.
2. An overview displays all activation codes already entered. This page also displays the serial number of the installed system.



3. Open the LANCOM Systems' registration page in a new window/tab (http://lancom.eu/en/service-support/registrations/software/large-scale-monitor/).
4. Select Product activation of the Large Scale Monitor.
5. Enter the serial number of the current system (see display in (2))
6. Enter the license number that you received at the time of purchase.
7. Click "Next >" to generate an activation code.
8. The activation code is displayed on the page (six groups with four characters per group).
9. Copy the license key into the field "Install new activation key:" and click "Install".
10. The code is loaded immediately and appears in the overview.

Continuous license check

The device "lsm-server" is automatically created during the installation and it monitors the server (see the section "Device "lsm-server""). The licenses installed on the server are also checked regularly (check LSM-Licenses). This check issues a warning if the server license is due to expire in 30 days or less, or if the number of configured devices exceeds 80% of the licensed number.

The situation becomes critical if the server license is due to expire in 7 days or less, or if the number of configured devices exceeds 90% of licensed devices.

5.21 Event console

Individual devices in a network issue so-called syslog messages, provided they are configured to do so, which is mostly done on the device itself. The event console receives and processes the syslog messages issued by the devices in line with the rules set out here.

Unlike the LSM that actively checks the devices, the event console receives the messages in a passive manner, displays the information and, depending on its configuration, will take action itself.

The event console processes the syslog messages from the devices in the sequence listed. Devices can, for example, be given a state, or messages can be sent or deleted.

If the archiving of messages is enforced in the event console configuration (see section "How to configure the event console" step (3)), all syslog messages received by the event console can also be viewed in the "event history" view. The other views offer lists that have been filtered already (see section 6.1.9 "Event console").

When installed, the LSM switches archiving of all messages on. Please refer to section 5.21.1 "The event console configuration" for further configuration options.

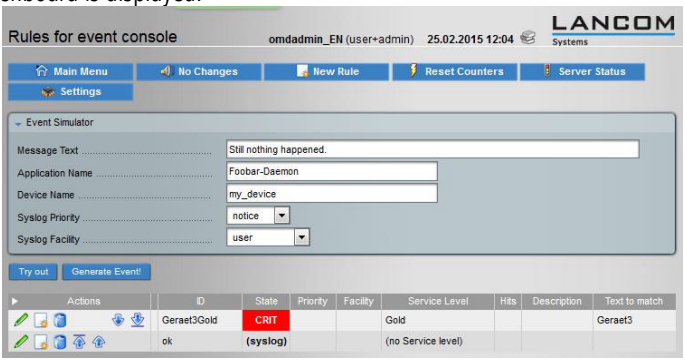
5.21.1 The event console configuration

In the configuration of the event console, you can specify its general behavior.

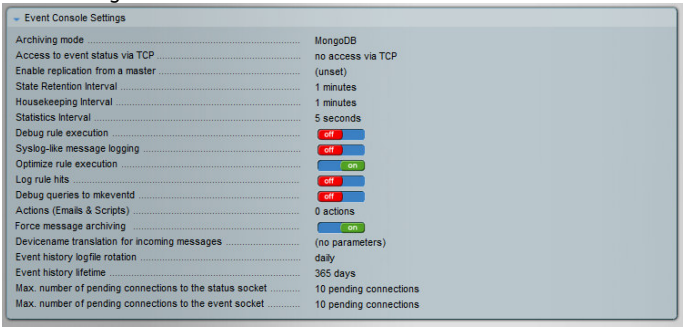
➢ From version 1.30, the event history lifetime is reduced to 30 days, also in the case of an upgrade from v1. 20. Because the search from the snap-in processes all of the entries in the event history, the original 365 days meant that this could take a disproportionately long time.

How to configure the event console

1. Select "Event Console" in the "CONFIG – Configuration" snap-in on the side bar on the main page.
2. A dashboard is displayed.



3. Click the "Settings" button.

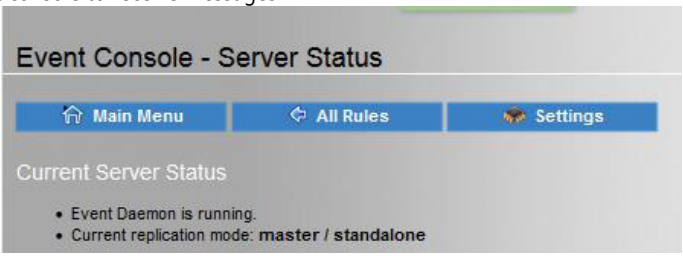


Here you can specify access to the messages, time periods, lifetime of the messages, and actions by the event console. If you wish to view all syslog messages in the event history, ensure that the "Force message archiving" option is set to "on".

4. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

Server status

"Server status" allows you to view the current activities. The event daemon needs to be running for the event console to receive messages.



Reset counters

This resets the counter for the relevant rules (see also "How to operate the event simulator").

5.21.2 Rules for the event console

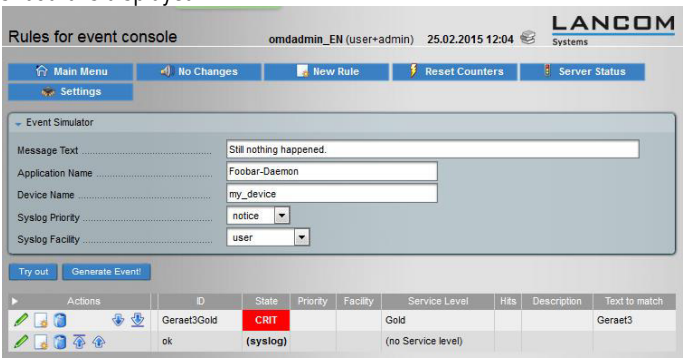
The event console can only present the incoming syslog messages in different views. It can also trigger actions.

Pre-installed rules

Four rules are already installed after installation. These map the syslog messages to the LSM-compliant states (OK, UNKNOWN, CRITICAL, WARNING). These rules do not perform further actions.

How to edit rules for the event console

1. Select "Event Console" in the "CONFIG – Configuration" snap-in on the side bar on the main page.
2. A dashboard is displayed.



3. The arrows  allow you to change the order of the rules.
4. Click on
   - the "New Rule" button to create a new rule.
   - Copy an existing rule with  .
   - Open an existing rule with  for processing or
   - delete a rule with  .

This opens the properties page for the rule:

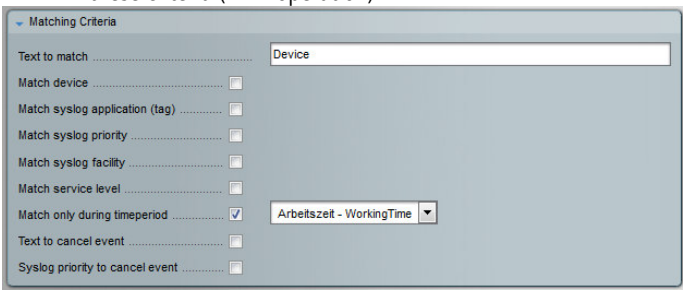
Here you can determine the properties of the rule.

- General properties

  Enter a unique ID and, if required, a description and whether this rule should be used now.

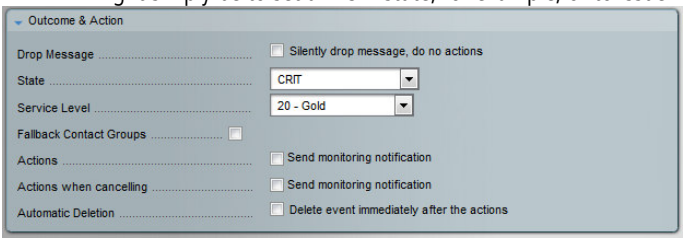
- Match criteria

  The criteria specified here check whether a syslog message needs to be examined by this rule. This may involve a simple inspection of the text, its origin (device), the priority, or a time period, as well as a combination of these criteria (AND operation).



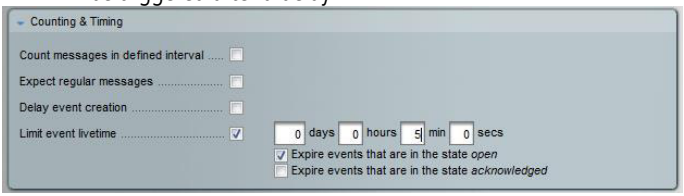
- Outcome & action

  If the above configured criteria all match, actions can be performed. This might simply be to set an LSM state, for example, or to issue notifications.



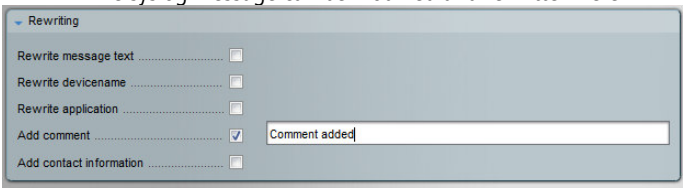
- Counting and timing

  Here the occurrence of syslog messages can be counted and actions can be triggered after a delay.



- Rewriting

  The syslog message can be modified and rewritten here.



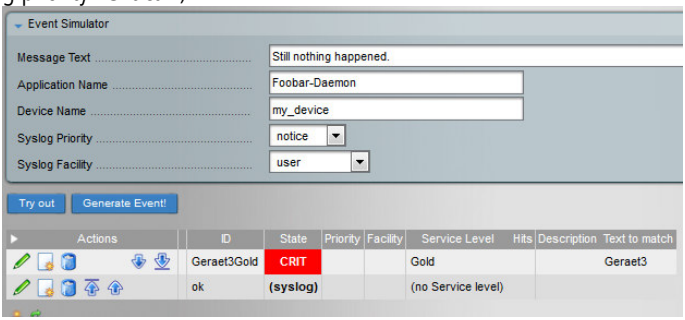
5. Close the configuration with "Save".
6. You can test the rule using the event simulator (see section "") before you enable it.
7. Any changes made still need to be enabled (see section 5.4.2 "Activating changes").

5.21.3 The event simulator

This simulator allows you to create an event, test the check, and evaluate the process.

How to operate the event simulator

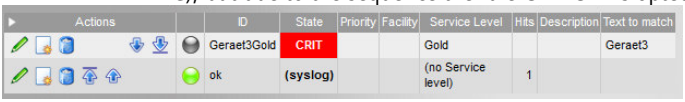
1. Open the event simulator in the Event Console configuration.
2. Specify what sort of event you would like to simulate (in this case a message with the syslog priority "Critical").



Then you can

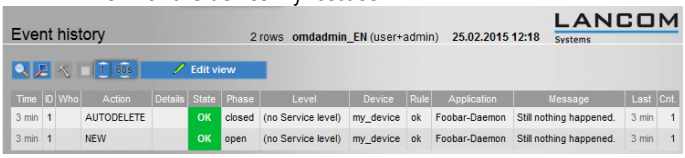
- Try out

  In this case, all rules are tested and the appropriate ones are highlighted in green. Hits are displayed. The hit counter can also be reset with the "Reset Counters" button.
  Example: In this case, two rules are applied first (CRITICAL and WATNING), but due to the sequence the rule CRITICAL is opted for.



- Generate event!

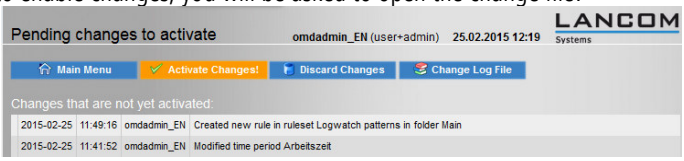
  In this case the event is simulated, i.e. an appropriate syslog message is sent. The rules are listed.
  Example: In this case the CRITICAL state is displayed in the "Event History" view for the device myhost089.



The event is then automatically deleted from the simulator.

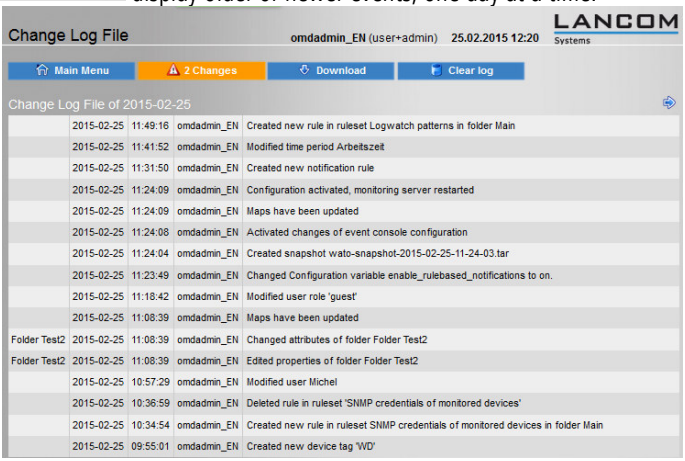
5.22 Change log file

If you want to enable changes, you will be asked to open the change file.



In this file it is possible to identify all changes that have been made since this file was last deleted.

The arrows  display older or newer events, one day at a time.



This file can

- be deleted.
- or saved Click “Download” . The file is saved as a CSV file with the name “wato-auditlog-<yyyy-mm-dd_hh_mm_ss>.csv to a local downloads directory.

You can view the next day with  , the previous one with  and the current one with  .

6 Display, views

The data gathered from the Large Scale Monitor can be processed and presented in a variety of ways.

The default installation package already contains a large number of different views. Where there are extra requirements, users can customize the way specific data is displayed.

For more information please refer to section 6.8 "Editing or creating views**".**

Only the Administrator has the rights to define new views for all users. It is possible to assign users rights to define their own views according to their role. For more information please refer to section 5.13 "Roles and permissions".

► All views displayed are always based on the overall scenario, known as the main directory. The name of the main directory is not shown in the title bar of the view, but the folder name is displayed when you are in a sub-folder.

6.1 Default views

The different views that are available are shown in the side bar. The views are organized in groups for a better overview.

The following groups of views are available:

- Dashboards

  The main dashboard is described in section 3 „The main page“. Please refer to section 6.9 "Creating and modifying dashboards" for further dashboard overviews.

- Devices

  Displays an overview of all devices in the network.

- Device groups

  All devices of the same model but in different folders are grouped by device type. A dashboard is displayed after the Administrator has combined devices into groups after installation.

- Checks

  Displays all checks and their results in detail.

- Check groups

  Displays the results of grouped checks, if the Administrator has combined checks in groups after installation.

- Problems

  This provides you with a detailed and descriptive display of problems that have occurred.

- Other
  An overview of different texts (e.g. comments or log files) is located here in addition to information on downtimes or other events.
- Event console
  Presents different displays of the syslog messages issued in the network.
- Inventory
  Provides information about the hardware and software of individual devices with an agent, e.g. the Linux server.
- WLAN + VPN
  This shows different views relating to LANCOM devices in the network.

The individual basic settings are explained below.

6.1.1 Limiting the number of entries displayed

The number of entries displayed in tables is limited to 1000. The display can always be expanded if more entries are available. The maximum number that may be displayed is 5000 entries in one table. Only a user with administrator rights can exceed this limit.

6.1.2 "Dashboard" views

The default page displayed here is described in section 3 "The main page". More dashboard overviews are explained in the section 6.9.1 "Pre-configured dashboards".

6.1.3 "Devices" views

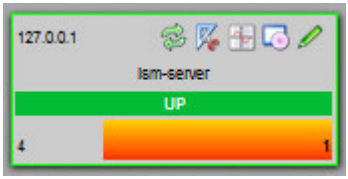
These views contain checks classified by different devices.

View	Explanation
All devices	Displays all devices as well as their device state. The following details are shown: • Device state (Up, Down) The tool tip on the device name displays the device's IP address. To view detailed information on the device, click the device name. This opens a new dialog box "Check of device…" • Device name • Device-dependent icons • State of last checks (OK, Warning, Critical, Unknown, Pending) Click the device names or the status number to view a detailed list of checks. • Result of check returns details of device status The following fields contain information that are only accessible for LANCOM devices via the "System information" check: • Name of the system The name of the LANCOM device that was assigned by the device administrator when configuring it. • Device name This device name is pre-defined by LANCOM • Firmware version Software version of the LANCOM device • Firmware dateDate of the firmware version

	• Serial number Pre-defined serial number of the LANCOM device • Location The location of the LANCOM device as configured in the device • Contact The contact configured in the device • VPN The number of VPN tunnels for which this device is a terminal. The field is left blank if the device does not support VPN tunneling. • Stations For WLAN devices, the number of currently logged-in WLAN stations. The field is left blank if the device does not support WLAN. • CONFIG folder The organizational or topological unit (folder) in which the device is located. This information is available for all devices.
All devices (tiled)	The individual devices are grouped as tiles containing device groups (see the section "Tile view").
All devices (Mini)	Provides a compressed, multi-column overview of the devices. The following details are shown: • Device state (Up, Down) The tool tip on the device name displays the device's IP address. To view detailed information on the device, click the device name. This opens a new dialog box "Check of device…" • Device name • Pro. The number of problems that have occurred, i.e. the number of checks that were not OK. Get detailed information by clicking on the number. • Stations The number of stations currently logged on.
All devices (WLAN-1)	Displays the same parameters as "All devices" but with the additional parameters describing WLAN-1. These parameters are only available for LANCOM devices. The fields are left blank if the device does not support WLAN or if the first WLAN radio module is disabled. The details of the views are as follows: • Stations Number of WLAN devices logged in via this access point. • Band The frequency band of the WLAN access point. • Ch. Number of the channel currently being used. • Tx Power Mean transmission power in dBm • Noise Noise of the signal on the channel. • Load Load on the channel • Bckg.Scan Background scan refresh rate configured in the device

All devices (WLAN-1+2)	Displays the same parameters as "All devices (WLAN-1)" but with the additional parameters describing WLAN-2. The fields are left blank if the device does not support WLAN, if it has no second WLAN radio module, or it is disabled.
Favorite devices	Shows all devices configured as favorites (see section 6.6.3 "Commands"). • Device state (Up, Down) The tool tip on the device name displays the device's IP address. To view detailed information on the device, click the device name. This opens a new dialog box "Check of device…" • Device name • Device-dependent icons • State of last checks (OK, Warning, Critical, Unknown, Pending) Click the device names or the status number to view a detailed list of checks.
Search devices	A search template appears here to help you search for devices. Select the appropriate search parameters from the drop down menu or select the required check box and launch the search by clicking "Search".

Tile view



Individual devices can also be displayed in tile form. This display format is available in the default configuration under "Devices | All devices (tiles)." The information is displayed as follows:

Place	Example	Explanation
Top left	127.0.0.1	IP address of device
Top right	Icons	Detailed information available, see section 6.3 "Check-specific icons".
Center	LSM server	Device name with a link to a display of the device status
Center	UP	This also shows the device status, in addition to the color of the tile
Bottom left	4	Number of checks that returned no problems. A list of checks that are classified as OK appears when you click on the linked number.
Bottom right	1	Number of checks that returned problems. A list of checks that recorded problems appears when you click on the linked number.

6.1.4 "Device groups" views

These views display any device groups within the network that were configured by the Administrator.

View	Explanation
Device groups	Displays the status of the devices in a multi-column table, grouped according to the configured groups. The following details are shown: • Device group • Status of the devices (UP, Down) • Device name Click the device name to view a detailed list of checks. This opens a new dialog box "Checks of device…." • Details Displays additional information on the checks specific to the check (icons) • Alias Alias of device, potentially a short description Click Alias to view detailed information on the device state. This opens a new dialog box "State of device…." • State of last checks (OK, Warning, Critical, Unknown, Pending) Click device names (new window "Check of device..") or the state number (new dialog box, e.g. "OK check of device…" to view a detailed list of checks that returned as OK.
Device groups (grid)	Shows the state of the devices in a multi-column table, grouped by the configured groups. The following details are shown: **Device group** • Device name Click the device name to view a detailed list of checks. This opens a new dialog "Check of device….". • Check state All checks performed are listed. They are highlighted with the color of the check status (OK – green, Critical – red, Warning – yellow, Unknown – orange, Pending – dark gray). • Icons Displays additional information on the checks specific to the check
Device groups (summary)	Shows a summary of the device groups in a multi-column table. The following details are shown: • Devices Click the device names to view a compressed overview of the checks on the individual devices in this group. This opens a new dialog box "Device group…." • Alias Device alias, optional short description • Device state UP, Down, Unknown, Pending • Check state OK, Warning, Critical, Unknown, Pending

6.1.5 "Checks" views

These show the views which are sorted according to the type and result of the checks.

View	Explanation
Checks with a change of status	Displays the checks whose state has recently changed. The following details are shown: • Device name • State • Check description • Result of check • Check-specific icons • Age Time or interval since this check state first occurred • Checked Time or interval since last checked
Checks by device group	Shows all checks, grouped according to the individual device groups. The following details are shown: **Name of device group** • Device name • State • Age Time or interval since this check state first occurred • Check • Check-specific icons • Result of last check
Checks of LSM	The Large Scale Monitor also monitors its own performance. All checks that are planned for the servers on which the Large Scale Monitor is installed are displayed here, grouped by servers. The following details are shown: **Device name (highlighted with the color of the check state)** • Status of check • Check • Check-specific icons • Result of last check • Age Time or interval since this check state first occurred • Checked Time or interval since last checked • Next check Time or interval until the next check • Perf-O-Meter

All checks	Shows a tabular overview of all checks that are currently configured in the system, irrespective of whether they are pending or have been performed. The view is grouped by device and the device is highlighted with the color of the current state. Here green represents OK, yellow is a warning and red indicates critical. The following details are shown: **Device name (highlighted with the color of the check state)** • Status of check • Check • Check description • Check-specific icons • Age Time or interval since this check state first occurred • Checked Time or interval since last checked • Next check Time or interval until the next check • Perf-O-Meter
Check_MK duration and latency	Shows the duration of the Check_MK checks and their latency. • State • Device name • Check (Check_MK) • Result of check • Check-specific icons • Age Time or interval since this check state first occurred • Checked Time or interval since last checked • Next check Time or interval until the next check • Perf-O-Meter • Duration Time span from sending the check to receiving the response, i.e. the duration measures the load on the network. • Latency Time span between planned and actual transmission, i.e. latency is a measure of the load on the server.
Favorite checks	The user can add favorite checks here. There are no examples here as favorites are specific to each user. (See section 6.6.3 "Commands")
Search checks	A Search template is provided which can be used to find individual checks. Refine the search parameters here by selecting keywords from the drop down menu and selecting the corresponding check boxes.

6.1.6 "Check groups" views

If the Administrator has grouped individual checks, e.g. the CPU utilization of several devices, information on these devices is displayed here.

View	Explanation
Check groups (grid)	Displays a table of the check groups. The following is displayed • Name of check group • Alias Description of group • List of checks e.g. in the form Device name ~ check
Check groups (summary)	Displays a very condensed form of the check groups. Displayed are • Name of check group • Alias Description of group • Summarized check state (OK, Warning, Critical, Unknown, Pending)
Check groups	Displays a table of the individual checked devices, sorted by the check groups. The following is displayed **Name of check group** • Device • State of the check • Check description • Result of last check • Check-specific details • Age Time or interval since this check state first occurred • Checked Time or interval since last checked • Check-specific icons

6.1.7 "Problems" views

Problems can be presented here to varying levels of detail. The following views are available:

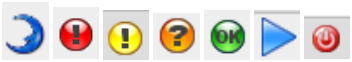
View	Explanation
Check problems per device	Displays the problems for devices that are not in downtime, grouped by device. The following details are shown: **Device name** • Check-specific icons • Check that was being conducted when problem occurred • Result of last check • Age Time or interval since this check state first occurred • Checked Time or interval since last checked • Next check Time or interval until the next check • Comments
Alert statistics	Provides an overview of any problems that have occurred. It displays the devices and the checks being conducted when the problem occurred, as well as the status (critical, unknown, warning), its frequency, and whether a correct status was restored (OK).
Pending checks	Shows the devices for which checks have been configured, but which have not yet been performed. Pending checks are grouped by device. The following details are shown: **Device name** • Pending check
Device problems	Shows devices where problems have occurred, i.e. the device state is “DOWN” or “UNREACHABLE”, grouped according to state. Displayed are **Device status** • Device name • Check-specific icons • Device state • Result of check • Identification of correct state prior to occurrence of problem • Type of problem identified (warning, critical, unknown) • Checks that are still pending, for which no result is yet available
Discovery problems	Displays the Check_MK-inventory checks that have caused problems. The display is grouped by state. **State** • Device

	• Check (Check_MK inventory) • Result of check • Age Time or interval since this check state first occurred • Checked Time or interval since last checked • Check-specific icons • Perf-O-Meter
Check problems	Shows the problem that has occurred and groups problems according to their status (critical, warning). The following details are shown **State of the check** • Device name • Description of the check being conducted when the problem occurred • Check-specific icons • Result of check • Age Time or time span since this check status first appeared • Checked Time or interval since last checked • Perf-O-Meter
Stale checks	Checks with stale results. **Device name** • State • Check • Result of check • Check-specific icons • Age Time or interval since this check state first occurred • Checked Time or interval since last checked

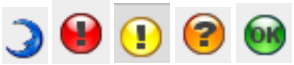
All displays are refreshed every 30 seconds.

6.1.8 "Other" views

Other additional views are also available e.g. views organized by comment, log file, etc.

View	Explanation
Device and check notifications	Displays all device and check notifications. The following details are shown: • Time or interval since entry was made • Contact Contact configured in the device • Event that triggered the notification. • Device where the event occurred. Linked to the checks for this device. • Check where the event occurred. • State State of device or check at the time of notification • Result of check or device state. • Information Informative part of the message • Type of state State (hard/soft/stopped/started)
Device & check events	Shows the different events for devices and checks grouped by time and date. The following details are shown: **Date** • Icon of the event e.g.  For a list of the icons see section 6.3 "Check-specific icons". • Time or interval since entry was made • Event Events are linked to a device or a check • Device name • Description of the check Where a check has led to the event. • Type of State State of device or check at this time (hard, soft, stopped, started, cancelled) • Check output Result of check or device state and information relating to it.
Global logfile	Shows all available events. The following details are shown: • Icon of the event e.g.  For a list of the icons see section 6.3 "Check-specific icons".

	• Time or interval since entry was made • Event Events are linked to a device (host) or a check (service) or are general checks. • Device name • Description of the check Where a check has led to the event. • Type of state at this time Indicates the state (hard, soft, stopped, started)
Comments	Shows comments throughout the system, grouped by device and checks. The following details are shown: **Type (device/check)** • Author Writer of the comment • Time When comment was created • Expires Date of expiry of comment • Type Type of entry e.g. reason that the entry was made: For a list of the icons see section 6.3 "Check-specific icons". • Comment text • Device Name of device for which the comment was entered • Check Description of check for which the comment was created • ID Comment's unique ID number
Search graphs	A Search template is displayed here to help you search for timeframe (graphs). Select the appropriate search parameters from the drop down menu or select the required check box and launch the search by clicking "Search".
Downtimes	Shows the scheduled and current downtimes, grouped by device and checks. The following details are shown: **Device/Check** • Device name Names the affected device. • Check description The check that is affected. • Downtime author Name of originator. • Downtime entry time Time or interval since the entry was made. • Downtime start time Time or interval since the start of the downtime. • Downtime end time Time or interval until end of downtime.

	• Downtime start mode A differentiation is made between fixed and flexible Fixed The downtime is defined for a fixed time and a fixed interval. Flexible This sets the duration of the downtime and a time range during which this downtime is started. The downtime begins during this time period, either the device itself goes down or a check returns a CRITICAL result. Once the downtime begins, the device is unavailable for the defined time period. • Duration The duration of the downtime. • Downtime comment Any comments on this event.
History of scheduled downtimes	Shows the log entries of past downtimes, grouped by device and checks. The following details are shown: **Device/Check** • Log: Icon of the event e.g.  For a list of the icons see section 6.3 "Check-specific icons". • Log: Time of the log entry Time of entry in the log file • Device name Names the affected device. • Check description The check that is affected. • Log: Type of state State (hard/soft/stopped/started) • Log: Output of the check plugin Indicates the result of the check

6.1.9 Event console

System messages received by the event console are displayed her.

For details on how to configure event consoles see section 5.21.1 "The event console configuration".

View	Explanation
Events	All events still open or in the "open" phase. • ID The row number in the event log file is used as the ID. It is linked to a more detailed representation of this event. • Icons Check-dependent icons • State • Level Service level assigned to this event. • Device Name of the device. . At the same time provides a link to the device's event sequence. • Rule ID of the rule relating to this event. • Application Institution responsible for sending the message • Message Text of the sent message • Last Time of the last occurrence • Cnt. Number of messages occurred
Event history	All syslog events received by the event console are listed here. • Time Displays the time from when the message is received • ID The row number in the event log file is used as the ID. It is linked to a more detailed representation of this event. • Who User performing the action. • Action Action that triggers the message or, as may apply, was triggered by it, depending on the phase • Icons Check-dependent icons • State • Phase

	An event can be open (1) or closed (2). Both are listed under the same ID. • Level Service level assigned to this event. • Device Device that sent the message. • Rule ID of the rule relating to this event. • Application Institution responsible for sending the message • Message Text of the sent message • Last Time of the last occurrence • Cnt. Number of messages occurred
Login events	All login events are listed here, i.e. all events with the "CONN-LOGIN_INFO" syslog tag. • State • Time Time of entry in the log file • Device Name of the device. Also provides a link to the device's event history. • IP address IP address of device • Message Text of the message • Prio Syslog priority
Statistic events	All login events are listed here, i.e. all events with the "PACKET_INFO" syslog tag. • State • Time Time of entry in the log file • Device Name of the device. Also provides a link to the device's event history. • IP address IP address of device • Message Text of the message • Prio Syslog priority
Syslog events	All events are listed here without further links. • State • Time

	Time of entry in the log file • Device Name of the device. • IP address IP address of device • Prio Syslog priority • Syslog function • Application Institution responsible for sending the message • Message Text of the message
WLAN events	All events containing WLAN in the message text are listed here. • State • Time Time of entry in the log file • Device Name of the device. . At the same time provides a link to the device's event sequence. • IP address IP address of device • Message Text of the message • Prio Syslog priority

6.1.10 Inventory

All devices are checked according to their hardware and software data. The results of the last inventorization are displayed here.

View	Explanation
CPU related inventory of all devices	All devices are checked and displayed here with their CPU and other performance data. "Availability" gives you an overview of the operational readiness of the devices. • Device The device name is linked to the comprehensive representation of the device's inventory. • Operating system • CPUs • Cores • Processor/maximum speed • CPU load Perf-O-Meter of the CPU load. • CPU utilization Perf-O-Meter of the CPU utilization
Software package search	Here you can search for devices or device groups with specific software packets installed. Alternatively you can search for software packets that are installed. The search results are set out in a table with the following details: • Device The device name is linked to the complete inventorization of the device's inventory. • Name Name of the software packet • Summary regarding the software packet • Version of the software packet • Packet version Sub-version of the software packet • CPU architecture • Type

6.1.11 "WLAN + VPN" views

These views contain details of the LANCOM WLAN devices. These devices provide a great deal of information on their configuration and state during checks.

View	Explanation
VPN tunnels	Displays VPN tunnels active in the network. • Device Device in the local network • Peer Device in the remote network • State Connected or not connected • Physical connection Shows the physical interface used to establish the connection. • Remote gateway Shows whether an additional gateway is used for the connection. • Connection time Indicates the time since the connection was established. • Last error • Mode Gateway mode (active or passive)
WLAN stations (all states)	Shows an overview of stations that are currently logged in to the various devices. The overview shows the following: • Device Click the device names to view the events for a specific device. This opens a new page "Station history of device <device name>". • Icons display additional information on the checks, specific to the check • MAC address of the logged in station. Click the MAC address to view the events for this device. This opens a new page "Station history of station <MAC address>". • IP address of the logged in station • Identification Provides a more detailed cleartext description of the WLAN station. This is stored in the device where the station is logged in. • Vendor • Interface The interface where this station is logged in to the device. • Key Encryption algorithm used on the WLAN line between the device and station. • Rx Data rate received by station in bytes per second

	• Tx Data rate transmitted by station in bytes per second • Signal Strength of signal in percentage rate. • WPA Encryption standard used. • State of connection (connected, authenticated, none, e1x-negotioation) • Network name Name of WLAN network where the device and station are located. • BSSID Basic Service Set ID, MAC address of the device (access point). • Age of the latest information
WLAN stations (connected)	Reduces the display of "WLAN stations (any states)" (see above) to the currently connected stations (state = connected).
WLAN station history	All events of the WLAN stations are displayed in chronological order. The following details are shown: • Device The tool tip on the device name displays the device's IP address. Click the device names to view the events for a specific device. This opens a new dialog "Check of device….". • Icons Displays additional information on the checks specific to the check • Time or interval since the event • MAC address of the logged in station. Click the MAC address to view the events for this device. This opens a new dialog "Station history of station ….". • Device manufacturer • Interface The interface where this station is logged in to the device. • Event Event that triggered the entry into the list. • Cause Specifies the cause of the event.

6.2 Links in the view

Links (URLs) are displayed at the bottom of the views.

	**URL to this frame** The context menu (right mouse-click) gives the option of displaying the current view without a sidebar in a new browser window or tab.
	**URL to this page including sidebar** The context menu (right mouse-click) gives the option of displaying the current view with a sidebar in a new browser window or tab.
	**Export as CSV** The currently displayed list can be exported as a comma-separated file (CSV). The format depends on the headings of the individual columns.
	**Add this view to...** The data displayed can be added to a dashboard. Further information about configuring dashboards can be found in the section "How to add the current view as a dashlet to a dashboard".

6.3 Check-specific icons

Additional information is available in several places within an overview. Clicking on an icon either runs the corresponding function or it displays more detail. A tool tip usually provides additional information on its function.

Icon	Explanation
	**Status** The "All Devices" view in this folder is opened.
	**Downtime** The device is unavailable (DOWN). This is a scheduled state.
	**Timeline** The tool tip shows a miniature view of the graphs. The time curve of the last hours is displayed here in graph form. This overview properties a smaller and a larger time window option.
	**Notifications** No notifications regarding this check are currently being transmitted.
	**Map** Indicates the location of a device on the stored map.

	**Reschedule passive** If this check is restarted, the associated active check is also restarted. This ensures that all other associated passive checks are restarted. A new check can be started with one click.
	**Reschedule active** Only this active check is started immediately, all other active checks are unaffected.
	**Acknowledged** Confirms that the problem has been acknowledged.
	**Log file** Opens the log file of the check or device.
	**Comment** The tool tip displays the last comment entered for this device or this check. Click to open the list of comments.
	**Changing configuration** The configuration tool for either the device or check (depending on the display) is opened. You can therefore make direct changes to the settings of the check. Please refer to section 6.8 "Editing or creating views" for further information.
	**Warning** Shows a problem, e.g. if a process cannot be restarted using “Reschedule”.
	**Flapping** The state of the device or check is changing very quickly.
	**Link to web GUI** The browser is directly linked here with the website of the LANCOM device. Please note that you must have the necessary access credentials at hand.
	**Active check is manually disabled for this device** This active check has been disabled. This icon can be deleted with “Commands”  using “reset information about modified attributes”.
	**Active check was enabled manually** This check was re-enabled e.g. after it had been disabled on the “Commands” tab. This icon can be deleted with the “Commands” button using “information about modified attributes”.
	**Edit parameters for this check** A new page is displayed with the rule associated with this check. If no rule has been created, you can now configure it for this device and set the desired parameters.

	**Log file** Linux and Windows devices create log files. These can be examined in more detail by using the log-data content analyzer. Please refer to section 5.17 "Log file content Analyzer" for further information.
	**Passive check is manually disabled for this device** This passive check was disabled e.g. on the “Commands” tab. . This icon can be deleted with “Commands”  using “reset information about modified attributes”.
	**Check state is stale**
	**Favorite** Devices and checks can be declared as personal favorites.
	**Device with agents** The inventory check can be performed for this device
	**Device for which the bulk discovery failed** Restart the bulk discovery (see the section "Discovering checks")

6.4 Global log file

The log file lists all events relating to the devices and checks. For a quick overview, the most important events are identified by an icon in the first column. Each row can also contain the following additional information:

The global log file is displayed by the view "Global log file" (see section 6.1.8 ""Other" views").

Icon	Explanation
	**Down or Critical** • The check returns the value “Critical”. • A device is in the “Down” state
	**Warning** The check returns the value “Warning”.
	**UP or OK** • The check returns the value “OK”. • A device is in the “Up” state
	**Unknown** The state of the device or check is not known.
	**Nagios** Indicates a restart by the underlying Nagios system.
	**Shutdown** Indicates successful shutdown of a device.
	**Flapping** The state of the device or check is changing quickly and is unstable.
Time	The associated time (as interval or date)
Event	The event that is the reason for the entry in the log file.
Device	The device associated with the check.
Check	The check that produced the event.
Type	State of device or check at this time (HARD, SOFT, STOPPED, STARTED, CANCELLED)
Result of check	Result of check or device state and information in relation to it.

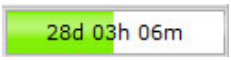
6.5 The Perf-o-meter

When a check returns a value, this is displayed in different views in the performance display (Perf-O-Meter). A number can be difficult to recognize, especially when it is embedded in explanatory text, so this display makes it much easier for the administrator to quickly identify significant values.

Click a Perf-O-Meter display to open a new dialog box with detailed diagrams representing recent values in graph form. In this way the time curve can be more accurately observed e.g. by viewing a time window (zoom).

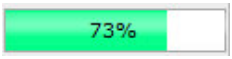
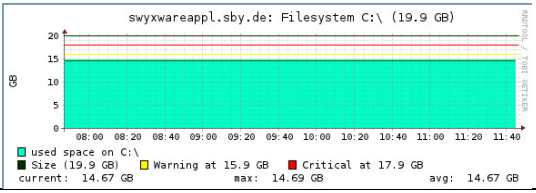
Absolute values

This displays the absolute parameter values on the scale.

Perf-O-Meter display	Diagram
	

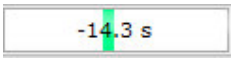
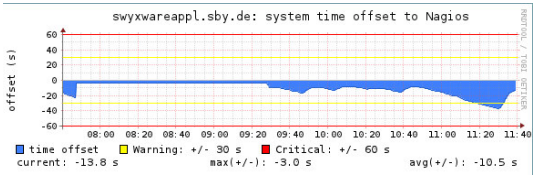
Percentage values

If the check is already returning a percentage value (e.g. CPU utilization, memory use), this value is displayed.

Perf-O-Meter display	Diagram
	

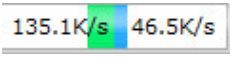
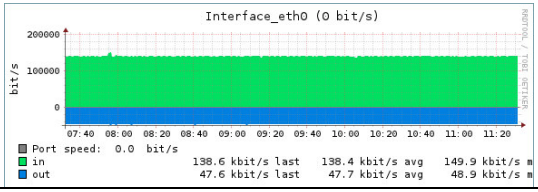
Positive / negative values

Where a value can be positive or negative, e.g. for comparing an offset, the zero-value of the axis is located in the middle of the display and the value can deflect to either side. For example, these values could be used to describe in-and outgoing traffic so that the sign indicates the direction.

Perf-O-Meter display	Diagram
	

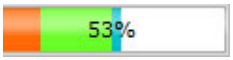
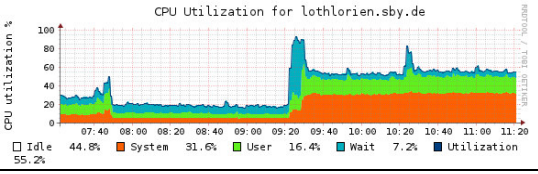
Two values

If the check returns two values (e.g. read and write or in and out) then, beginning in the middle, one value will also be represented to the left and the other value to the right.

Perf-O-Meter display	Diagram
	

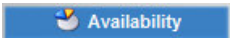
Multiple values

If the check returns multiple values, the display will be graduated in color, in the same way as the display in the diagram.

Perf-O-Meter display	Diagram
	

6.6 The Views menu bar

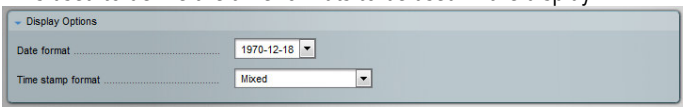
Views can also be customized to a greater level of accuracy as per user requirements.

	**Filters** Refinement of the view. See section 6.6.2 “Filters”
	**Display** The time format is specified in the display here. Please refer to section 6.6.1 "Display" for further information.
	**Commands** Executes commands on checks and devices, see section 6.6.3 "Commands"
	**Check box** Allows individual rows to be selected, see section 6.6.4 "Mark with "X"".
	**Number of columns** Clicking increases this up to max. eight columns.
	**Refresh rate in seconds** Clicking changes the display refresh rate. Available values are 30s, 60s, 90s, and "Off".
CONFIG 	**Configuration** Leads to the configuration of devices, etc..
Edit View 	Opens the dialog to edit the current view (see 6.6.5 "Edit View")
Availability 	"Availability" provides you with an overview of the device's operational readiness (for example see section 6.6.6 "Availability").
Map 	Opens the dialog containing the stored maps, (see section 5.5.13 "Edit map").

These buttons may not be useful for every view and there are special filters and commands for certain views to refine what they display even further.

6.6.1 Display

"Display"  is used to define the time formats to be used in the display.



Date format

Select your required date format here. You can choose between the following formats:

- YYYY-MM-TT 1970-12-18
- DD.MM.YYYY 18.12.1970
- MM/DD/YYYY 12/18/1970
- DD.MM. 18.12)
- MM/DD 12/18

Time stamp format

- Mixed

  Alternates between the relative and absolute time stamp.

  Example: 14hrs or 31.01.2012 06:17:48
- Absolute

  The date and time are in the defined format.

  Example: 31.01.2012 06:17:48
- Relative

  This shows the time elapsed since the event and the current time. Depending on the duration, either hours (hrs), minutes (min) or seconds (s) are used.

  Example: 14 hrs or 117 min
- Both

  Both time formats are shown, first the absolute date followed by a hyphen and then the elapsed time.

  Example: 31.01.2012 06:17:48 – 14hrs
- Unix time stamp (epoch)

  Number of seconds since 1 January 1970, 0 hours (UTC)

6.6.2 Filters

You can use filters to further customize the current view to meet your requirements. Click on "Filter" 

The view can be restricted to a folder or subfolder. Additional filter options are available and can be defined in detail. The criteria input here are used when generating the view (see section 6.8 "Editing or creating views").

Click "Search" after specifying the criteria to apply the filter to the current view.

You will know that the current view is being filtered if the "WARNING" () icon appears in the menu bar. Click on the WARNING icon if you would like to change the current filtering. The filter options open up again.

You cannot save filters for later use. If you wish to use a filter in the long-term, edit the view and save it under a new name.

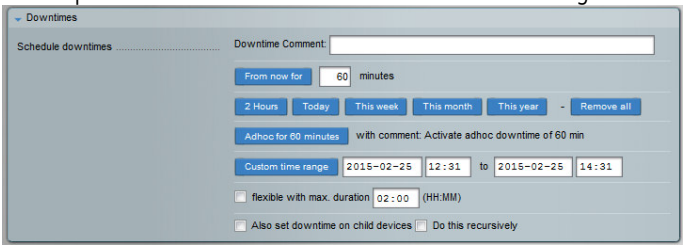
6.6.3 Commands

The views of "Devices" and "Checks" feature the "Commands"  icon. Commands can be sent to all or a selected number of devices or checks here.

See section 6.6.4 "Mark with "X"" for how to select individual devices.

Current downtimes

The devices selected here are set to the DOWN state. This allows times and periods to be selected. You are required to enter a comment about the downtime configuration.



- From now for x minutes

  The downtime starts for the given period.

- Suggested time periods

  You can select from 2 hours, today, this week, this month and this year. Use “Remove all” to delete all scheduled downtimes.

- Ad hoc for 60 minutes with the comment "Activate ad hoc downtime of 60 min".

  The time and comment are specified in the global settings for the LSM (see section 5.8.6 "LSM status GUI").

- Custom time range

  The period within which the downtime is to take place can be defined here.

- Flexible with max. duration

  A flexible downtime with a maximum duration can be configured here in hours and minutes.

- Also set the downtimes for child devices

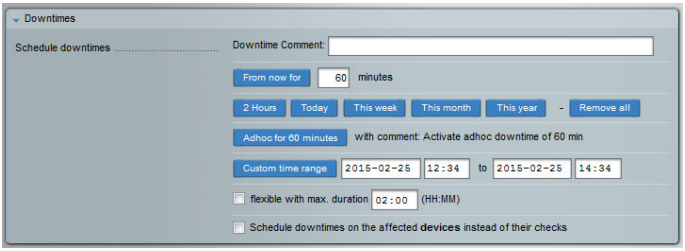
  This also includes devices that directly depend on the devices shown here (parent relationship).

- Do this recursively

  This also includes all devices depending on the devices shown here (parent relationship).

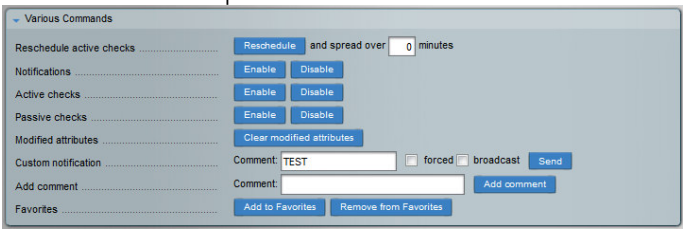
Configuring downtime for checks

Downtimes can also be scheduled for the checks. This means that the check is not performed at this time.



Various commands

You can set which action should be performed here.



Details of the available options are as follows:

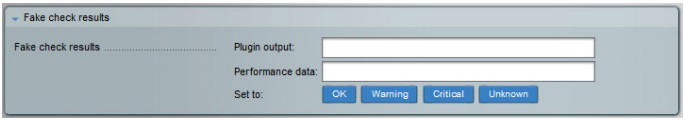
Category	Options
Reschedule active checks	All active checks can be immediately restarted here.
Notification rules	The notifications for this check can be enabled or disabled here.
Active checks	The active checks themselves can be enabled or disabled here. Disabled checks are denoted by  while re-enabled checks are represented by 
Passive checks	Passive checks, i.e. checks that are initiated by active checks, can be enabled or disabled here.
Modified attributes	Reset the information about modified attributes. Removes the  icon that indicates that an active check has been manually disabled.
Custom notification	The device is prompted to send a message to its relevant contact group. Enter the message text in the "Comment:" field. It is also possible to define here who the message is sent to: • Forced Ignores any limitation due to time periods and sends the message anyway. • Broadcast The message is sent to all this device's contacts, with the exception of those who have been excluded. Click "Send" to send the message immediately.

Add comment	This comment is added to all devices selected with this command. This is saved by clicking on "Add comment"
Favorites	All devices selected with this command are either added to or removed from the favorites.

Fake check results

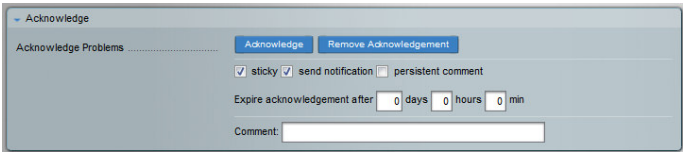
You can set the check result to the desired value (Up, Down, Unreachable). The result modified here is applicable until the next check is performed.

An appropriate message for the log file can be stored here. The performance data can also be faked here.



Acknowledge

A warning can be confirmed here or a confirmation that has been sent can be retracted. A confirmation cannot be sent without a comment. Unless they have been configured otherwise (see below), the confirmation and comments are retracted when the state changes, e.g. if a Warning becomes Critical or vice versa.



- Persistent
  The confirmation and comment are maintained until the state changes to OK. They are then deleted.
- Send notification
  A notification is sent to all relevant administrators.
- Persistent comment
  The comment entered with the confirmation is permanently maintained.

Time limit on acknowledgment

Acknowledgment can be limited to a certain time. If zero is entered here, this time is unlimited.

6.6.4 Mark with "X"

Using the "X" command  , a column with a check box is displayed in front of the first column. Clicking again causes the column to disappear again. Any marks that have been set are preserved.

In the title check-box column you will see another "X"  . Clicking on this icon marks either all the check boxes of the relevant group or deletes all tags of this group again.

The procedures configured under "Commands" can then be applied to the devices selected here.

The selection of individual devices or checks is possible only if the user can execute other commands on the device.

Configuration of "X"

By default the check boxes are not displayed. If a user has already modified the configuration in a particular view, i.e. has made the check box visible or invisible, this setting is maintained for the user and stays the same regardless of changes to property settings of a view (see section 6.7 "Properties of a view").

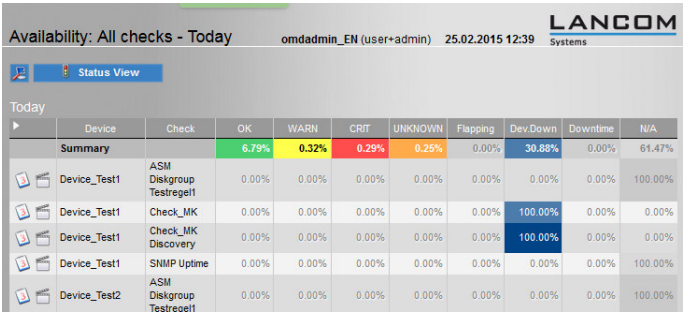
6.6.5 Edit View

If the user logged on has the right to create new views or modify existing ones, then the "Edit view" button is enabled. This opens the "properties of a view" page. The currently selected view can be modified here or a new view can be created, by saving the view under a new, unique name. Please refer to section 6.7 "Properties of a view" for further information.

6.6.6 Availability

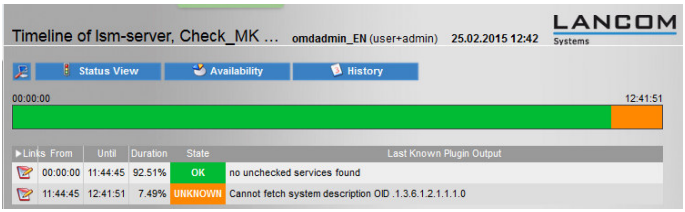
In some views, such as with "All Devices", you can use the "Availability" command.

This command opens a new view that displays all devices and their availability.



Device	Check	OK	WARN	CRIT	UNKNOWN	Flapping	Dev.Down	Downtime	N/A
Summary		6.79%	0.32%	0.29%	0.25%	0.00%	30.88%	0.00%	61.47%
Device_Test1	ASM Diskgroup Testregel1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%
Device_Test1	Check_MK	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%
Device_Test1	Check_MK Discovery	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%
Device_Test1	SNMP Uptime	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%
Device_Test2	ASM Diskgroup Testregel1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%

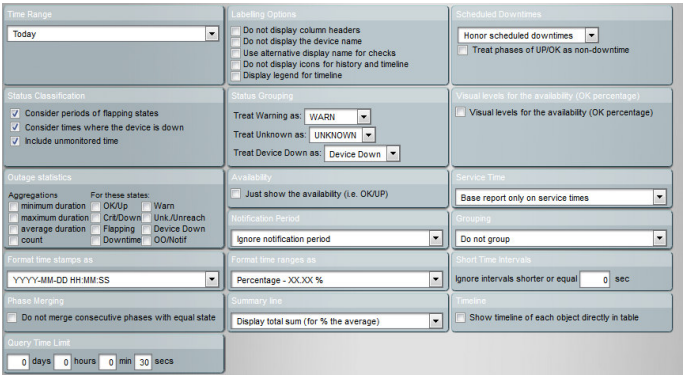
Click on the  icon to open a time bar and table with detailed information on availability for this device.



The "Event history" command or the  icon provide you with an overview of the event history for this device.

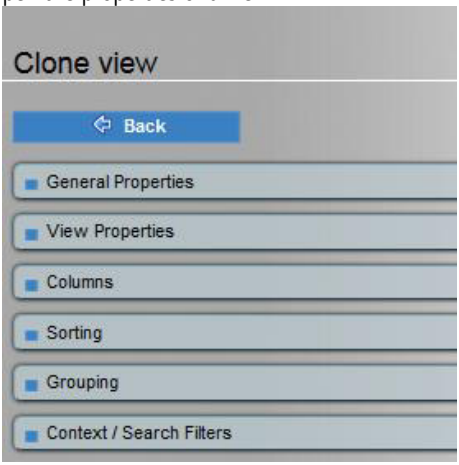
Configuring the Availability

The icon  invokes the configuration of the availability. Here you can specify the time ranges, groupings or threshold values in detail.



6.7 Properties of a view

The individual properties of a view are explained here. Provided you have the appropriate permissions, you can change existing views or create completely new ones.
Click on "Edit View" to open the properties of a view.



General properties

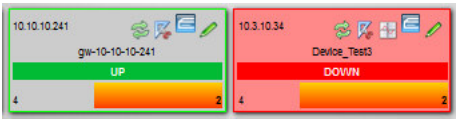
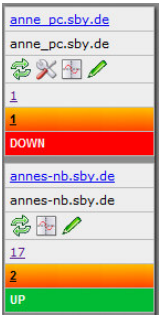
General details relating to the view are found in the upper section.

Category	Explanation
Information for a single object	This type is given during creation and cannot be subsequently modified; there are single and multiple objects.
Unique ID	The ID is used in URLs that point to a view, e.g. `view.py?view_name=myview.` It is also used internally to identify views. You can create several views with the same title, but only one per ID. If you create a view that has the same ID as a built-in view, then your view will overwrite that (shadowing it).
Title	**Name of view** This designation is used everywhere, e.g. in the side bar, etc.
Topic	The view configured here appears later in the side bar under this directory.
Description	A longer description of the check can be saved here.
Button text	The text that appears on the buttons is defined here. Please use only a small number of characters.
Button icon	Select one of the icons here if one is also required on the button.
Visibility	The visibility is set with the check boxes • Hide this view from the sidebar • Do not show context buttons for this view

	• Make this view available to all users

View properties

Further properties of the view are to be found here.

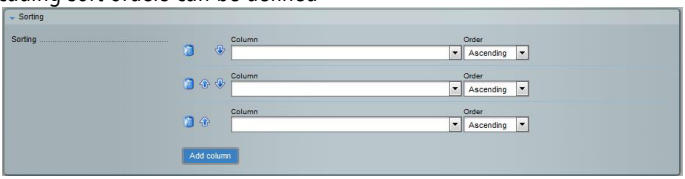
Category	Explanation
Data source	The source of the data for this view is named here.
Options	• This view is available for mobile devices. • Show data only on search • Always display check boxes Check boxes shown for each device can be used to select individual elements (see section 6.6.4 "Mark with "X""). • Make view sortable for users If this option is selected, each column header has a link. Click this link and the view changes so that the display is sorted by this parameter. Sort order is ascending (alphabetically) or following a double-click descending (alphabetically). • Play alarm tones If the check box is selected alarm tones will be played if there is any change to the state currently displayed (Down, Critical, Unknown, None).
Automatic page reload	Define how often the page should be reloaded. If you prefer the page not to be automatically reloaded, leave the field blank or enter a 0.
Basic layout	The following options are available: • Table This generates a basic table view • Tiles The individual devices are represented as tiles.  • Balanced boxes The column width is adjusted to fit the longest entry. • Single dataset Each dataset (i.e. a row in the table) is condensed to a single column table. 

	• Mobile: Dataset The “Mobile dataset” display is optimized for mobile devices such as smartphones. • Mobile: List A one row list is shown, optimized for mobile devices. • Mobile: Table The “Table” display is optimized for mobile devices.
Number of columns	A multi-column display is also available for narrow views (with a small number of parameters). Enter the number of columns for the entire display here.
Column headers	Here you can set whether a column heading is displayed once per group, is repeated every 20 lines, or not displayed at all.

Sorting

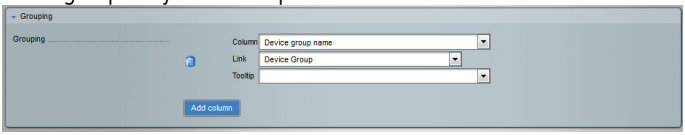
The criteria used to sort the display are defined here. Select the sort parameter in the drop-down menu and set whether sorting should be in ascending or descending order.

Multiple cascading sort orders can be defined

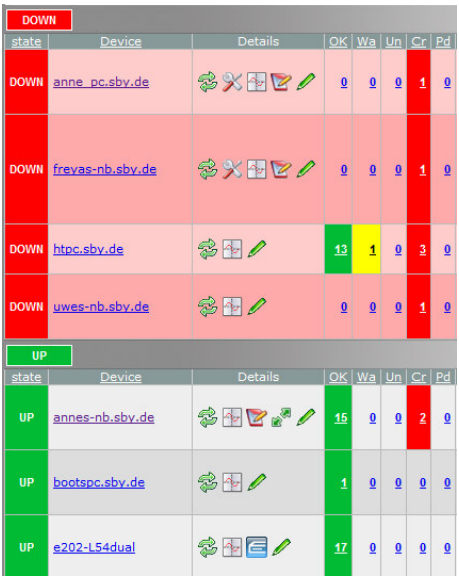


Grouping

The display can be grouped by individual parameters.



A clear division will then appear in the display and the group will be assigned its own heading with the parameter contents. If for example you group by device state, a list is generated with the group of devices that are DOWN displayed at the top, followed by the group that is "UP".



► Please note that you must also sort in accordance with these criteria (in the example: "Device state"). Otherwise multiple groups will be displayed.

Using "Link" you can define if and how the group name is to be linked. You can also assign the matching tool tip which will be displayed when the cursor is placed over the heading.

Use the "Add column" button to add further criteria for grouping. These are also listed in the group heading.

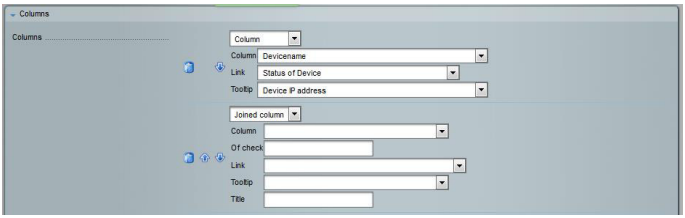
You can delete a parameter using  . The order of the grouping parameters can be modified using the  arrows.

Columns

In this section it is possible to define which of the checked parameters are to be displayed in this view.

Using "Link" you can define how the displayed parameters are to be linked. You can also assign the matching tool tip which will be displayed when the cursor is placed over the heading.

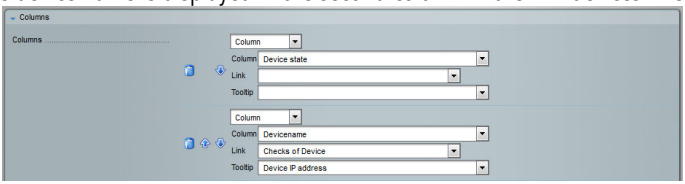
If you would like to display information here determined by checking a device, select a "Joined column" and enter the name of the check.



Use the "Add column" button to add another column to the view. You can delete a column using  . The order of the columns can be modified using the  arrows.

Example:

The device name is displayed in the second column in the "All devices" view.

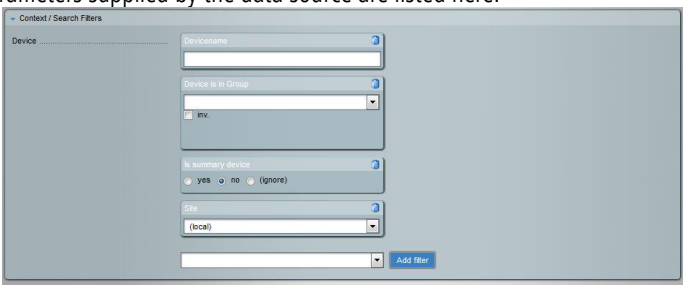


This name is linked with a new view "Checks of device" which opens when you click on it.

At the same time, the device's IP address is displayed when you move the cursor over the device name.

Context / search filters

All of the parameters supplied by the data source are listed here.



You can decide whether the parameter should be used for further filtering of the data. Select additional filters from the drop-down list or delete the one shown.

Try out and Save

Use “Try out” to preview the changes to the current view. It is displayed directly below the configuration table. If you exit the view without saving it, the old configuration is retained.

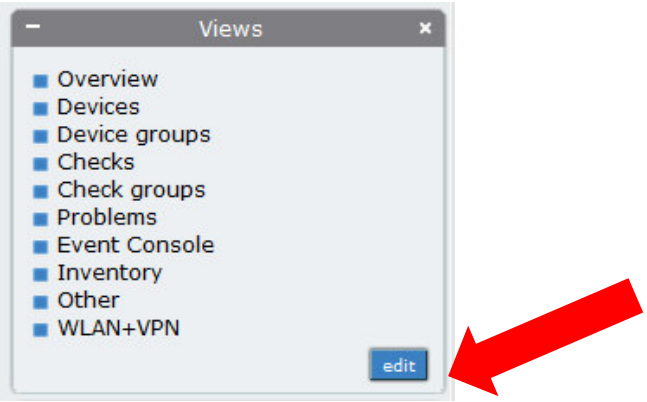
➢ NOTE: If you store the modified view here using “Save” it will be saved with the same name. If you wish to save the current changes under a new name, enter a unique new name for this view in the “Title” field and for the one-time ID.

6.8 Editing or creating views

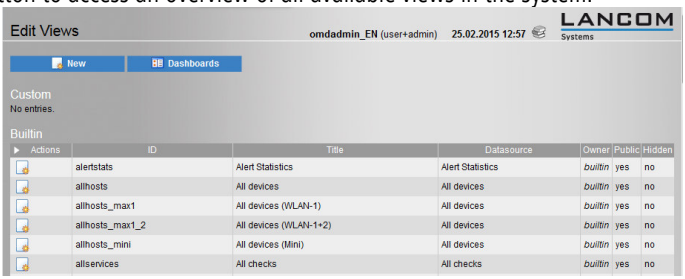
Completely new views can be configured based on existing views. An existing view can be completely redesigned or a completely new view can be created.

The user must have administrator rights to configure new views. Please refer to section 5.12 "User" for further information.

Users with the right to define new views will see the “Edit” button in the “Views” category on the side bar.



Click this button to access an overview of all available views in the system.



6.8.1 Built-in views

The built-in views only offer the option in the first column to create a clone  . They cannot be edited.

If a view is modified using  , this view is then saved again under the same name, and in this case the options "Delete"  , "Clone"  and "Edit"  now appear in the last column. Whenever this view is selected, the customized view is opened.

The standard views cannot be deleted.

➢ NOTE: If there is a modified view with the same name as a built-in view (usually created following the customization of a built-in view), this will be the version displayed when this view is selected in the side bar.

6.8.2 Customized views

Views that have already been customized offer the following options:

- Delete  this created view.
- Clone  , i.e. create a new view based on the current one. It is essential that a new unique name be assigned to this new view.
- Edit  , i.e. the current view is modified.

How to modify an existing view

1. Click "Edit" in the "Views" category in the side bar to open the overview of all available views.

   The "Edit views" page opens in the main window.

2. Select an existing view and click on "Clone"  . A new view is created.
3. This opens the properties of a view.

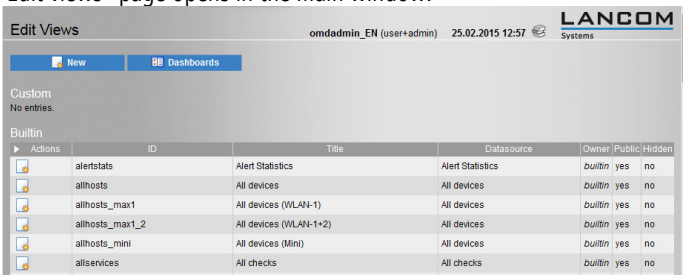
   Customize all the view properties according to your requirements. Please refer to section 6.7 "Properties of a view" for further information.
4. You can preview the modified view.
5. Click "Save" to store your changes.

   Your new customized view is then created.

How to create a new view

1. Click “Edit” in the “Views” category in the side bar.

   The “Edit views” page opens in the main window.



   This shows a list of all views, the integrated (supplied) ones and the user-specific ones already created and made generally available.
   Click the "New" button at the top of the screen.

2. In the drop down menu, select the data source that is to be the basis for the new view. Several data source options are available.
3. Click "Continue".
4. This opens the option to select the object type.

   Select the context type from the selection list. The list stems from the data source selected earlier. With the type "Multiple*", a reduced number of context buttons is available as this is a summary of several devices, etc. Considerably more information is available with the "Single*" type.

5. Click "Continue".
6. This opens the properties of a view.

   Customize all the view properties according to your requirements. Please refer to section 6.7 "Properties of a view" for further information.

7. You can preview the modified view.
8. Click “Save” to store your changes.

   Your new customized view is then created.

6.9 Creating and modifying dashboards

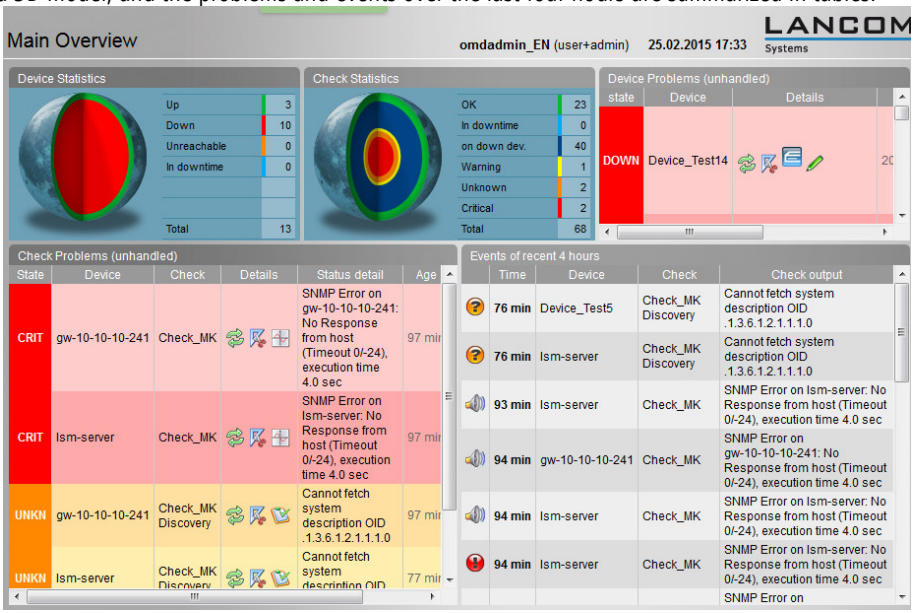
A dashboard is a particularly visual way of understanding the situation in the selected folder. It can be summarized as tables, graphs or other displays highlighted in color. Dashboards providing different overviews are supplied. Existing dashboards can be modified by moving or replacing the individual items, referred to as dashlets. You can also create your very own customized overviews.

6.9.1 Pre-configured dashboards

As of v1. 20, a number of dashboards are installed by default, which are known as the built-in dashboards.

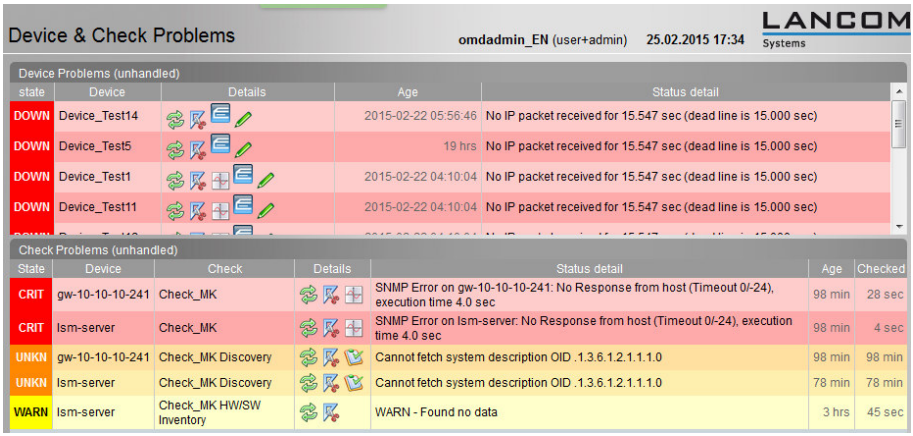
Main overview

This dashboard provides a rapid overview of all of your device and check statistics in the form of a 3D model, and the problems and events over the last four hours are summarized in tables.



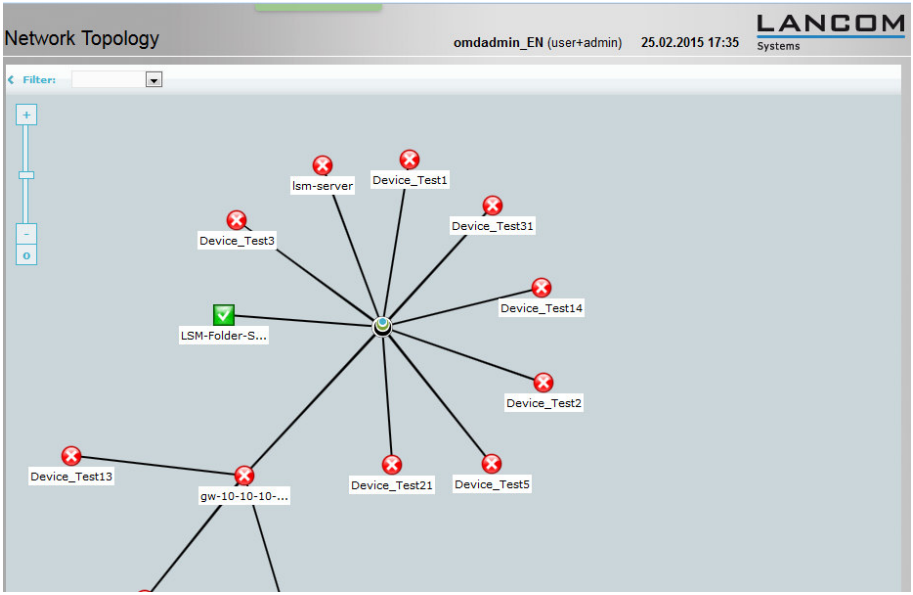
Device and check problems

This dashboard provides two tables displaying the device and check problems.



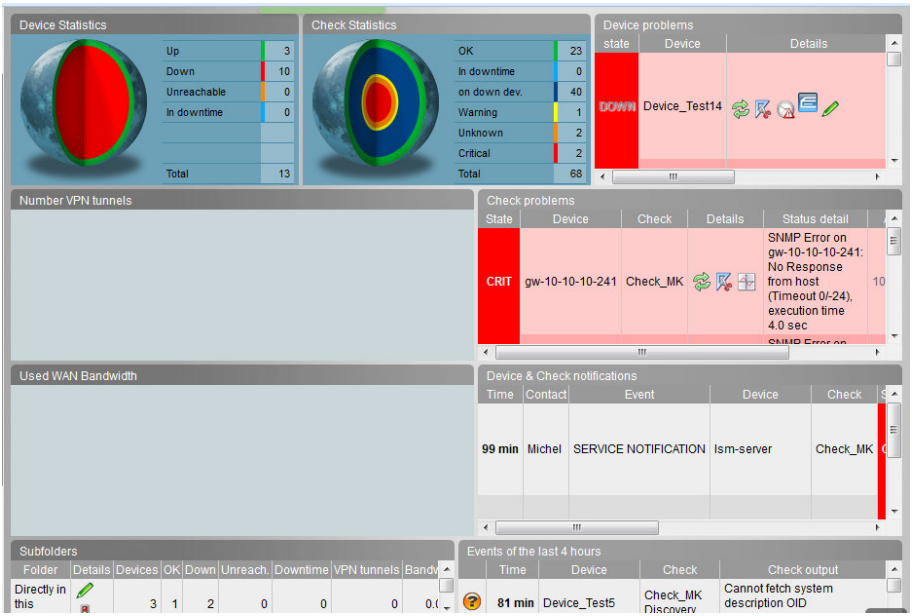
Network topology

The networks is mapped out here on the basis of the available data. This allows you to very quickly identify active devices and to interpret their hierarchical dependencies, such as those determined by means of a parent scan. By moving the mouse over an item in this view you receive comprehensive status information about the device.



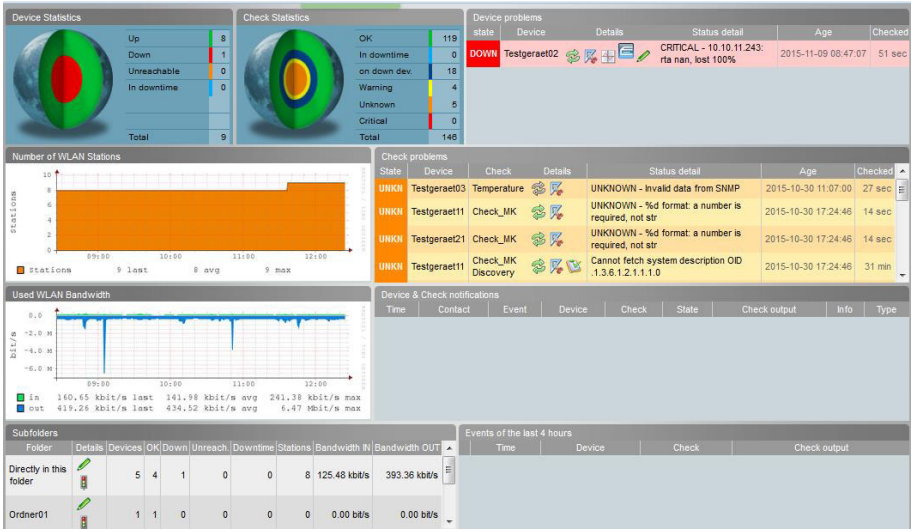
VPN

This main overview shows your device and check statistics in the form of a 3D model, and the problems and events over the last four hours are summarized in tables This dashboard has been enhanced with two graphs displaying the data about the VPN connections (number and bandwidth) over a time.



WLAN

Here you will find the "Device and check problems" dashboard, i.e. two tables, a graphical display of information about the WLAN, including the number of stations and the bandwidth used, and also information about notifications.



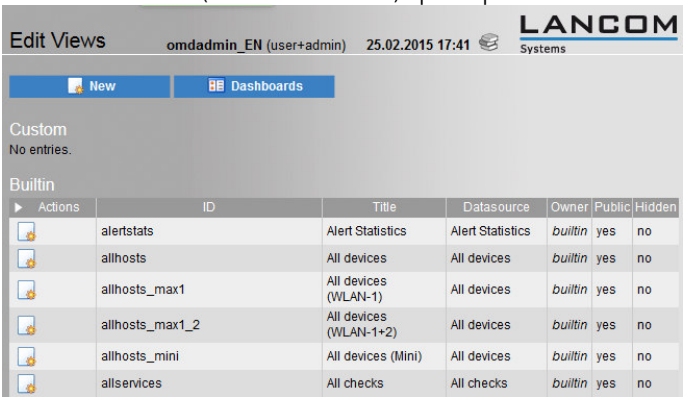
6.9.2 Properties of a dashboard

A dashboard is a special view, i.e. the properties are similar to those of a view. Provided you have the appropriate permissions you can change existing dashboards or specify completely new ones.

How to edit the properties of a dashboard

1. In the "Views" snap-in click on the "Edit" button. If this button is not visible, then you do not have the necessary permissions. Contact your administrator about this.

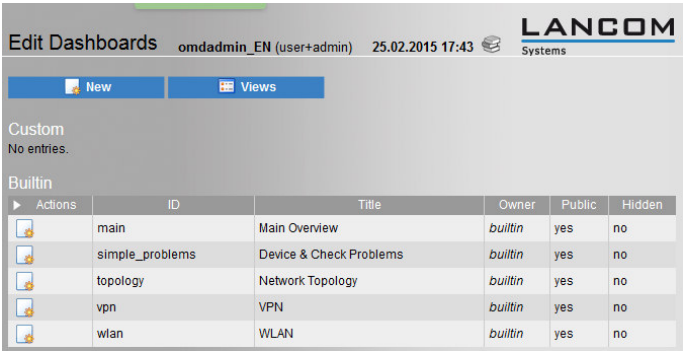
   An overview of the views (built-in and custom) opens up.



Actions	ID	Title	Datasource	Owner	Public	Hidden
	alertstats	Alert Statistics	Alert Statistics	*builtin*	yes	no
	allhosts	All devices	All devices	*builtin*	yes	no
	allhosts_max1	All devices (WLAN-1)	All devices	*builtin*	yes	no
	allhosts_max1_2	All devices (WLAN-1+2)	All devices	*builtin*	yes	no
	allhosts_mini	All devices (Mini)	All devices	*builtin*	yes	no
	allservices	All checks	All checks	*builtin*	yes	no

2. Select the button "Dashboards" button here.

   You will see a list of the dashboards On display are the built-in dashboards and any custom dashboards that were created.

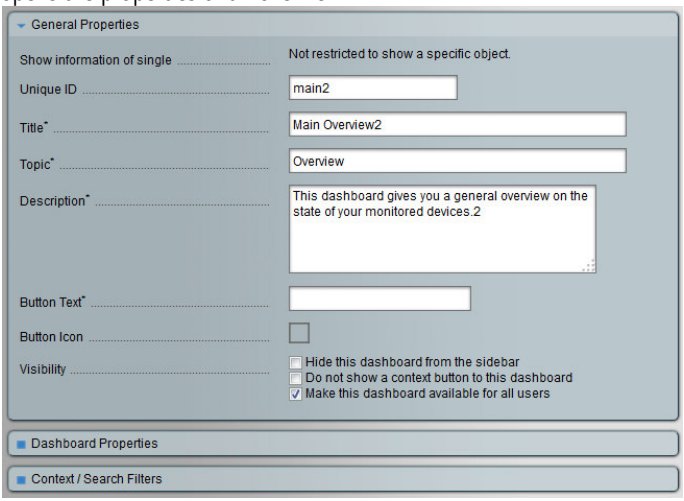


Actions	ID	Title	Owner	Public	Hidden
	main	Main Overview	*builtin*	yes	no
	simple_problems	Device & Check Problems	*builtin*	yes	no
	topology	Network Topology	*builtin*	yes	no
	vpn	VPN	*builtin*	yes	no
	wlan	WLAN	*builtin*	yes	no

3. You have several options:

- Delete  a dashboard. This is only possible with custom dashboards.
- Clone  , i.e. create a new dashboard based on the current one. It is essential that a new unique name be assigned to this new view. If this is not the case, the built-in dashboard is replaced by the modified one.
- Edit  , i.e. the current overview is modified.

This opens the properties of an overview.



4. Here you can set the name, description, icon and button text, and set the visibility, and under "Context / search filters" you can define a range of filters.
5. "Save" creates and displays the new dashboard in the sidebar snap-in, provided it was configured this way.

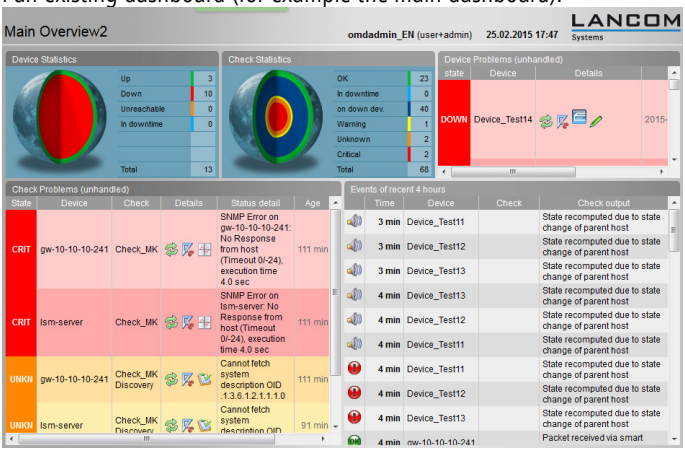
   Now you can start adapting the dashboard to your wishes by changing, deleting or adding individual items (dashlets) (see the section "How to edit a dashboard")

6.9.3 Editing dashboards

You can edit existing dashboards by moving, deleting or adding individual dashlets. The built-in dashboards are not deleted, they are merely replaced by custom dashboards of the same name. If custom dashboards are renamed or deleted, the built-in ones are displayed again.

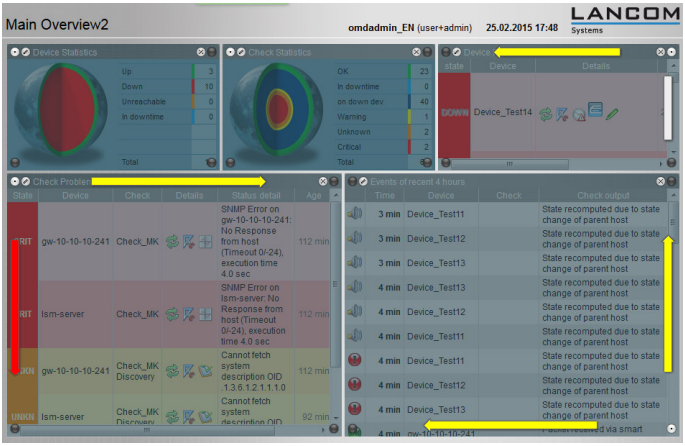
How to edit a dashboard

1. Open an existing dashboard (for example the main dashboard).



2. Swap to the editing mode by moving the cursor to the bottom right-hand corner of the main dashboard. Click on the button that appears there 
   The menu appears.
3. Select "Edit Dashboard".

The main dashboard appears in editing mode.



4. All individual items, the so-called dashlets, appear with the editing icons and can now be modified.

Icon	Explanation
	**Edit dashlet** This opens the properties for this dashlet. You can modify these now. See the section "How to edit the properties of a dashlet".
	**Delete dashlet** You can now discard this dashlet. This removes it from the main dashboard.
 enabled  disabled	**Anchor dashlet** When the icon is active, the rectangular dashlet is anchored at this corner (default: upper left). Changes to the size of the display window originate from this corner. The other corners are disabled (gray).
  	**Change the size of the dashlet** These arrows move out from the anchor icon and show in which direction the dashlet can be resized. • If the arrow is yellow, the size is changed in such a way as to use the available space without hiding another dashlet. • If the arrow is red, the maximum size in the browser is adopted, possibly leading to overlapping with other dashlets. • A light gray bar indicates that the size is fixed. The size can be altered by dragging with the mouse, just as with a window, but only on the edges opposite the arrows. You can swap between the different states by clicking on the arrow.
Cursor buttons	**Move dashlet** A dashlet can be moved via drag&drop over the available space.

5. Change the dashboard to meet your requirements.

6. Finishing reviewing by selecting  "Stop Editing" in the menu at the bottom right-hand corner.

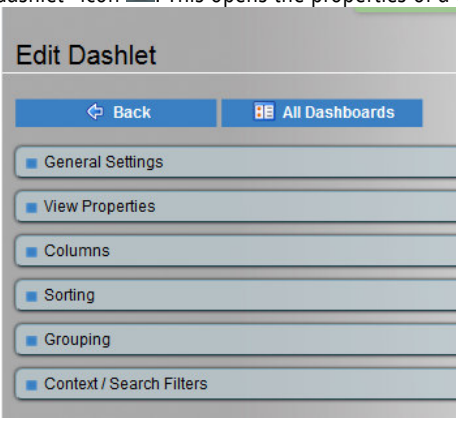
Edit dashboard items (dashlets)

Each dashboard is composed of a variety of dashlets. You can create these yourself or select them from existing ones and adapt them to your requirements.

How to edit the properties of a dashlet

If you are in a dashboard's editing mode (see "How to edit a dashboard"), you can edit the properties of a single element.

1. Select the "Edit dashlet" icon  . This opens the properties of a dashlet..



Many dashlets provided are views that have been adapted to the dashboard, so the properties you find here are like those for the views as described in section 6.7 "Properties of a view". The properties shown depend on the dashlet that you selected, and this example lists the properties of a table.

- General settings

  You specify general settings such as title bar, a link, or the background color here.

- View properties

  You will find the data source, the layout, and the update interval here.

- Sorting

  You can specify sorting by column contents here.

- Grouping

You can specify specific grouping according to column contents here.

- Columns
  You specify which columns are to be displayed here.
- Context / search filters
  Special filters can be specified here.

2. With "Save" you return to the dashboard in editing mode.
   You can now configure or add additional dashlets.

How to add the current view as a dashlet to a dashboard

1. You have a view on display. Beneath the view there are various links.
2. Select "Add this view to..."  .
   An list of all dashboards is displayed.
3. Select the dashboard to which you would like to add this view.
   You now see this view in editing mode and the view can be seen as a dashlet on the dashboard.
4. You can now continue to edit the dashboard and position the dashlet (see the section "How to edit a dashboard").

How to add new dashlets

1. If you are in a dashboard's editing mode (see "How to edit a dashboard"), you can also select further dashlets via the menu in the bottom right-hand corner  and add them to your dashboard.
   Various dashlets are available.

Icon	Explanation
Existing view	Here you can create a dashlet from an existing view. All of the available views are offered for selection.
View	You can create a new view here. Please refer to section 6.8.2 "Customized views" for further information.
Performance graph	You can configure the graphic display for a device or check here.
Device statistics	Device statistics are displayed in a 3D image in this dashlet.
Check statistics	This dashlet displays check statistics in a 3D image.
Custom URL	A URL can be entered here, the content of which is displayed in this frame.
Static text.	A static text entry can be displayed on the dashboard here.

2. Select the desired dashlet and configure its properties (see "How to edit the properties of a dashlet").
3. Once you have configured all the dashlets, you can position them on the dashboard.

4. From the menu at bottom right-hand of the screen, select the  "Properties" and give the dashboard a new name.

5. Finish overall configuration by selecting  "Finish Editing" in the bottom right of the menu.

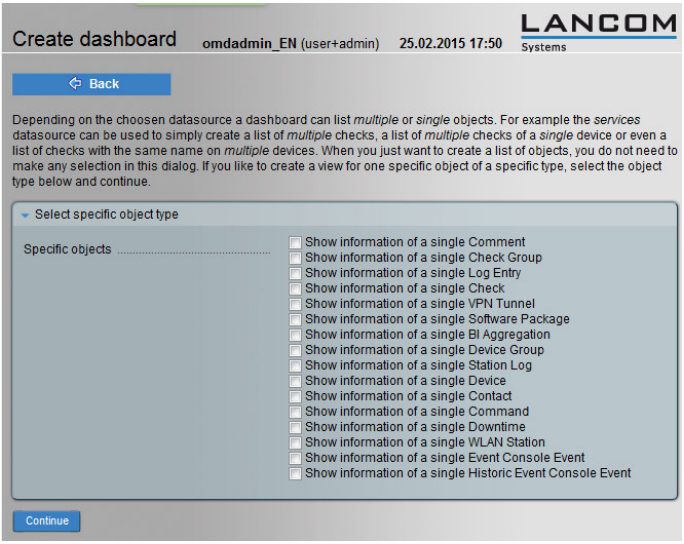
6.9.4 Recreate dashboard

Instead of altering an existing dashboard, it is often easier to create a new one and then add and position the dashlets .

How to create a new dashboard

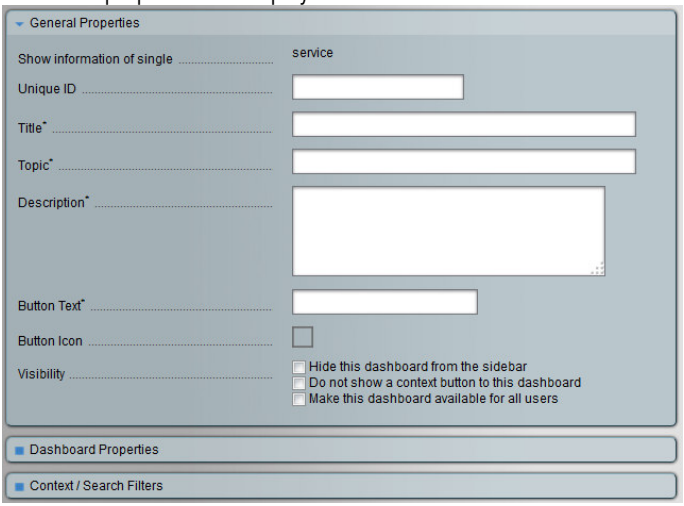
1. Select the "Edit" button in the "Views" snap-in and switch to the dashboard view.
2. Select the creation of a new dashboard with "New".

   The "Create dashboard" page is displayed featuring the "Select specific object type" menu.



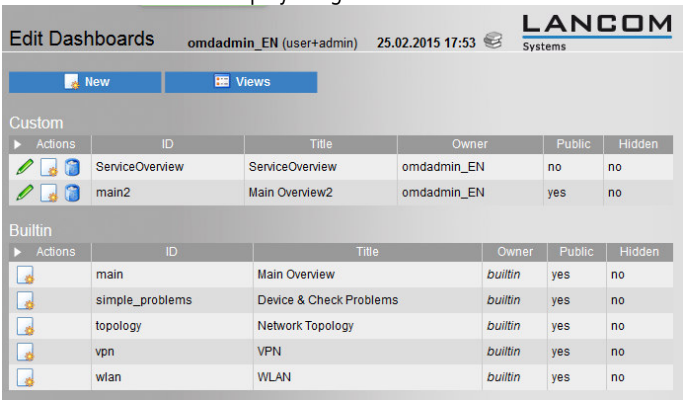
3. Select the object type from the list and click on "Continue".

The dashboard properties are displayed.



4. Here you enter at least the ID and a title.
5. Conclude your entries with "Save".

   The list of all dashboards is displayed again.



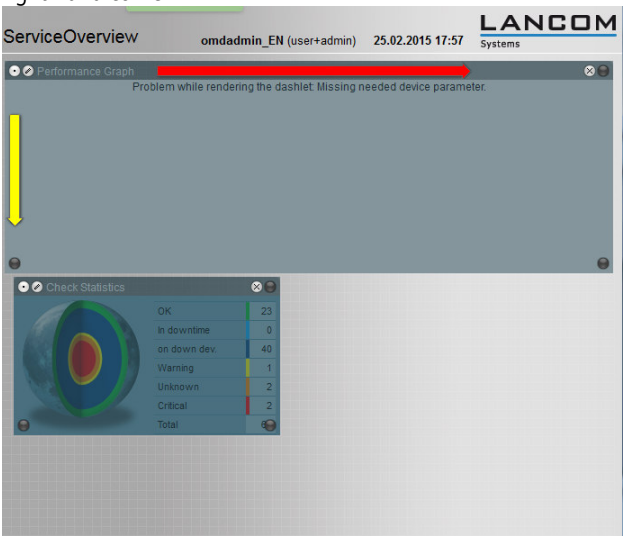
6. Click on the title of the new dashboard you have created.

   An empty page opens.

7. Select "Edit Dashboard" from the menu  in the bottom right-hand corner.

A grid interface appears.

8. Now you add dashlets by once again selecting "Add dashlet" from the menu in the bottom right-hand corner.



9. If you have configured and positioned all of your dashlets, stop editing again in the bottom right of the menu .

7 Snap-ins

Various snap-ins are located in the side bar on the left side of the Large Scale Monitor user interface. Snap-ins are small modules with a variety of information and display options that can be added to or deleted from the side bar as required. The relative position of a snap-in in relation to the other snap-ins can be changed. Configuration of the side bar is user-specific.

7.1 Snap-ins in the basic installation

The snap-ins in the basic installation are explained below.

7.1.1 Overview

The standard setup features the following snap-ins in the side bar.

Snap-in	Description
Tactical overview	Shows the number of devices being monitored, the number of individual checks, the number of the problems it encountered, and the number of unhandled cases. Please refer to section 7.1.2 "Tactical overview" for further information.
Search	Helps to search for devices. Please refer to section 7.1.3 "Search" for further information.
Folders	Shows an overview of the folders that have been created. By selecting a folder, you display the entry that is highlighted under "Views" (e.g. All devices) relating to this folder and its subfolders in the main section (2). Please refer to section 7.1.4 "Folders" for further information.
Views	Lists the different views available. Here, you can determine which view you want to see on the right-hand side. The view you select here always relates to the area selected under "Folders". Please refer to section 7.1.5 "Views" for further information.
LSM Links	Provides a map overview of the various folders for the entire network. Please refer to section 7.1.6 "LSM Links" for further information. There is also an option here to display the Large Scale Monitor manual.
CONFIG - Configuration	Opens the Large Scale Monitor's configuration program. Please refer to section 7.1.7 "CONFIG – Configuration" for further information.

How to reposition the side bar

To reposition the side bar click on a free area of the side bar. Keep the mouse button pressed and move the side bar either up or down, or use the scroll bar to the right of the side bar.

Hide and show side bar

You can hide the side bar by clicking in the snap-in field on the left-hand side of the LSM window. Display the side bar again by clicking on the left frame.

7.1.2 Tactical overview

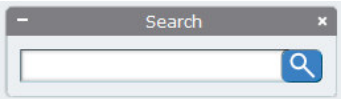
This is an overview of the current state of the devices and checks.

Click one of the areas shown to open a corresponding view containing detailed information. The details shown are as follows:

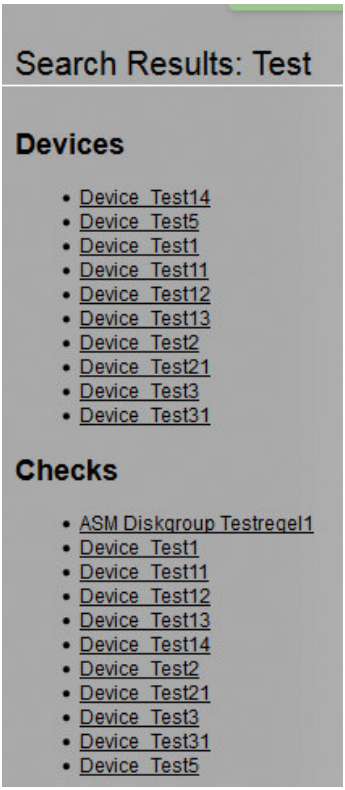
	On display	View and Check
Devices	The number of devices currently being monitored.	All devices (See section 6.1.3 " "Devices" views")
Problems	with how many devices have problems arisen.	Device problems Filter Device state = DOWN, UNREACH (See section 6.1.7 ""Problems" views")
Unhandled	The number of these problems that have not yet been confirmed, i.e. those with the "unhandled" status.	Device problems "Device problem has been acknowledged" = "no" filter (See section 6.1.7 ""Problems" views")
Checks	how many checks have been performed.	All checks Filter check state = All (See section 6.1.5 ""Checks" views")
Problems	the number of checks with problems.	Check problems Filter check states = WARNING, CRITICAL, UNKNOWN (See section 6.1.7 ""Problems" views")
Unhandled	the number of these check problems that have not yet confirmed.	Check problems Filter problem acknowledged = no (See section 6.1.7 ""Problems" views")

7.1.3 Search

You can search for devices, checks, WLAN stations, VPN tunnels, and MAC or IP addresses here.



The search result is displayed in groups. You can then use the links to open further views for the search term.



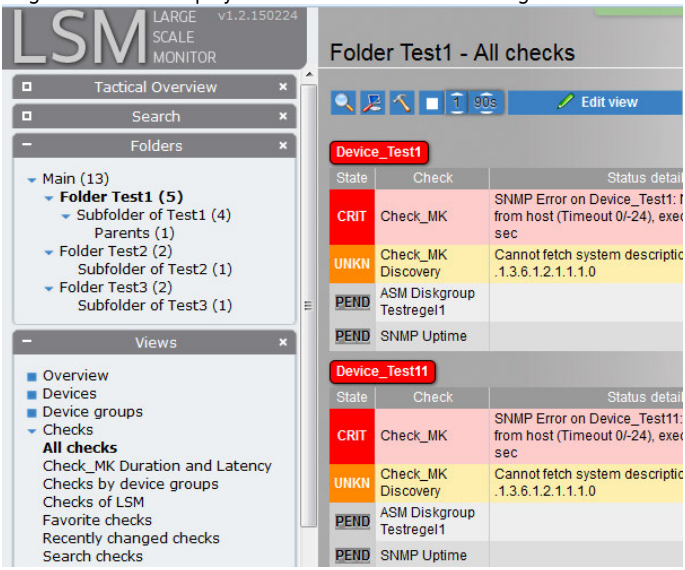
➢ From version 1.30, the event history lifetime is reduced to 30 days, also in the case of an upgrade from v1. 20. Because the search from the snap-in processes all of the entries in the event history, the original 365 days meant that this could take a disproportionately long time.

7.1.4 Folders

This snap-in menu displays the structure of the monitored network. The displayed view is linked to the selected folder, i.e. the displayed view always refers to the active folder.

Example:

Select a folder (here: "test 1 folder"). The folder is highlighted (in bold). Select the view to be applied to this folder (here: "All checks"). The view is also marked in bold. The right-hand side displays the "All checks" view relating to the folder "Folder Test1".



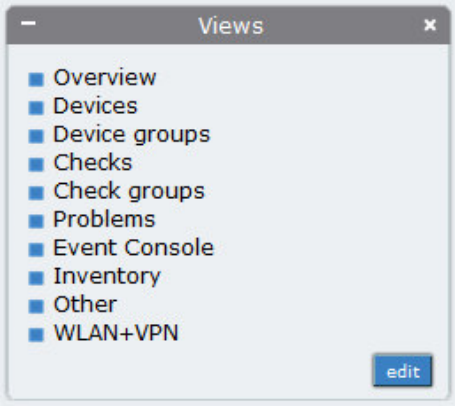
For the same folder you can then select another view, e.g. "favorite checks", or apply the same view for a different folder, e.g. "folder test 2". The active view is highlighted (bold).

The folder structure shown here was defined during configuration (see section 5.5.8 "Creating folders") and can of course be continuously added to and expanded.

7.1.5 Views

This snap-in displays all of the views that are available to the users. They are grouped in a logical manner. Click ■ to open the sub-folders or click ▼ to close an open sub-folder.

The view displayed in the right-hand window always refers to a folder that is also highlighted in the "Folders" snap-in (also see section 7.1.4 "Folders").

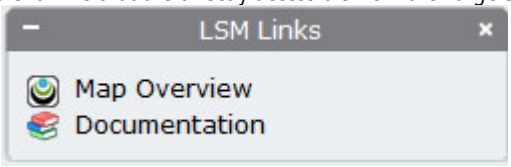


Additional information on the different views is available in section 6 "Display, views".

If you have the right to edit views, you can create a new view with "Edit" here. The ”Edit views” page opens in the main window. Please refer to section 6.8 "Editing or creating views" for further information.

7.1.6 LSM Links

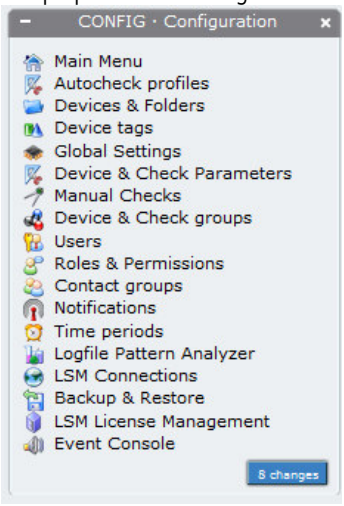
This contains the different links that are directly accessible from the Large Scale Monitor.



Icon	Name	Explanation
	Map overview	Contains maps that are integrated during configuration. These maps reflect the organizational structure. It shows all of the individual devices. Please refer to section 5.5.13 "Edit map" for further information.
	Documentation	This contains all the Large Scale Monitor documentation in PDF format, which can be opened directly in the main window via the browser.

7.1.7 CONFIG – Configuration

This is where you can configure all properties of the Large Scale Monitor.



	Name	Explanation
	Main menu	Overview of all configuration options. For more information, please refer to section 5 "Configuration".
	Autocheck profiles	Autocheck profiles are used to speed up the bulk check discovery if your network contains many similar devices. This is where you create the autocheck profiles and edit them. For more information, please refer to section 5.6 "Autocheck profilesDisplay, views".
	Devices & folders	Here you are able to edit, change and extend the entire structure of the installation, as well as to add and move devices. For more information, please refer to section 6 "Display, views".
	Device tags	Define new device properties (tags) here. This value of a tag is then specified as a parameter. For more information, please refer to section 6.7 "Properties of a view".
	Global settings	Configure the general settings here. For more information, please refer to section 5.8 "Global settings".
	Device & check parameters	Parameters are assigned to the individual devices and checks here. For more information, please refer to section 6.7 "Properties of a view".
	Manual checks	Here you create your own rule sets for the checks, if the bulk discovery produced checks that are not to be used. Please refer to section 5.10 "Manual checks" for further information.
	Device & check groups	Devices and/or checks are grouped here and the parameters are set for these groups. For more information see section 6.1.4 ""Device groups" views" and section 6.1.6 ""Check groups" views".
	User	Edit users and their properties here. For more information, please refer to section 5.12 "User".
	Roles	User roles and their associated permissions (Edit, Show, Delete, etc.) are defined here. For more information, please refer to section 5.13 "Roles and permissions".//////////////////////////////
	Contact groups	Contacts that have been created can be added to groups, for example to receive notifications. For more information, please refer to section 5.14 "Contact groups".
	Notifications	Rules are used to control the way in which notifications are sent. These rules can be configured here. For more information, please refer to section 5.15 "Rule-based notifications".
	Time periods	Define the intervals within which a specific event should occur. For more information, please refer to section 5.16 "Time periodsTime periods".
	Logfile pattern analyzer	Windows and Linux devices create log files while they operate. The content of these log files can be further processed by the Analyzer with the use of rules. For more information, please refer to section 5.17 "Log file content Analyzer".

	LSM connections	The Large Scale Monitor can also collect data from different systems and over dispersed locations. For more information, please refer to section 5.18 "LSM connections".
	Backup & restore	Configurations can be backed up and restored when required. For more information, please refer to section 5.19 "Backup & restore".
	LSM License Management	Manage the different Large Scale Monitor licenses here. For more information, please refer to section 5.20 "LSM License Management".
	Event console	The LSM can evaluate syslog files and initiate rule-based actions. For more information, please refer to section 5.21 "Event consoleEvent console".

7.2 Edit snap-ins

You can edit the existing snap-ins or add new snap-ins to the side bar from an existing set.

	Click this icon in the snap-in's title bar to minimize the snap-in. The snap-in is minimized, the title row remains in the side bar.
	Click this icon in the snap-in's title bar to restore the snap-in.
	Click this icon in the snap-in's title bar to remove a snap-in from the side bar.
	To add a snap-in, click on this icon in the menu bar at the bottom of the side bar.

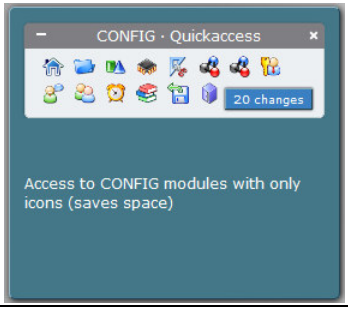
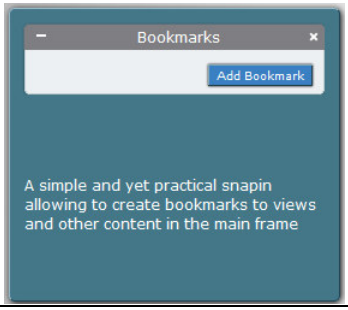
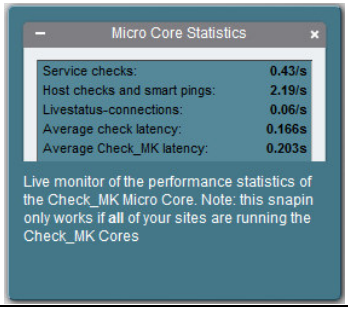
7.2.1 Move snap-ins

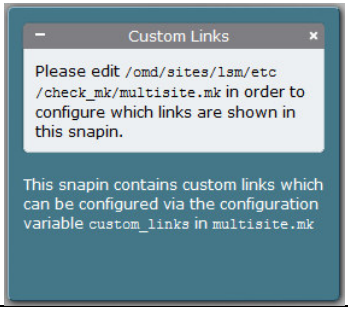
The individual snap-ins can be moved within the side bar using Drag&Drop. To do this, click in the title bar of the snap-in and keep the mouse button pressed. Drag the snap-in to the desired position and release the mouse button again.

7.2.2 Add more snap-ins

To add a snap-in, click on this icon  in the menu bar at the bottom of the side bar. It opens an overview of the available snap-ins in the main window. Click on one of these snap-ins to insert it. It is immediately display in the lowest position on the side bar.

7.3 Overview of additional snap-ins

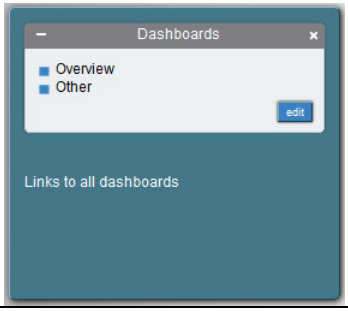
	**CONFIG Quickaccess** This item gives experienced administrators space-saving and quick access to the various configurations.
	**Bookmarks** Links to individual displays can be easily and quickly added. When the display for bookmarking is in the main window, just click on "Add bookmark". The link is inserted immediately. The page is displayed in the Large Scale Monitor's main window. With  you can edit the displayed name and the link itself. A bookmark is deleted by clicking on  .
	**Micro core statistics** Current monitoring of the Check_MK Micro Core performance data. NOTE: This snap-in can only be used if the Check-MK Micro Core is active. Please refer to section 4.5 "Changing the monitoring core" for further information.



Custom links

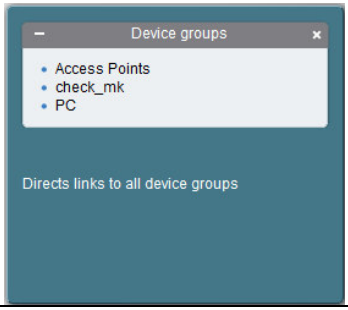
Links to other external websites must be preconfigured. They will then be available here.

This type of link is configured by the administrator by editing the /omd/sites/lsm/etc/check_mk/multisite.mk file.



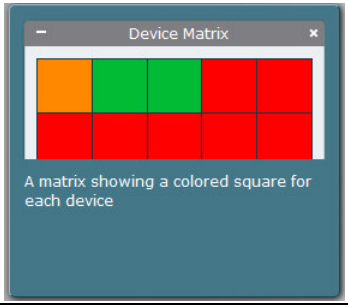
Dashboards

Different dashboards are available for quick access.



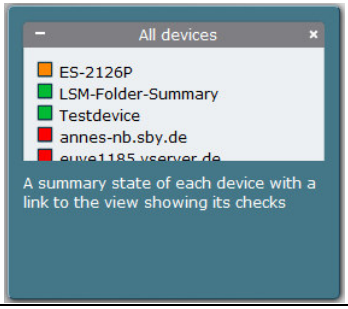
Device groups

This snap-in offers a direct link to each device group.



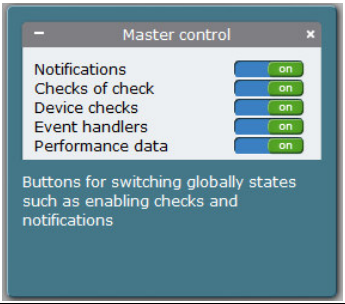
Device matrix

All devices are displayed in the form of a colored tile in the side bar. The tool tip menu displays the name of the device. Click on a device to display the checks for this device in the main window.



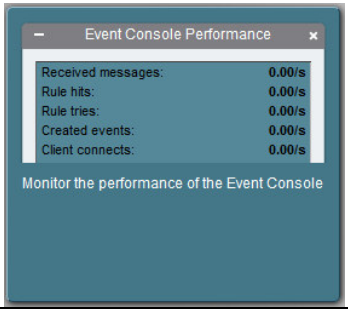
All devices

All devices are listed here. The colored itemization symbol denotes the device status. Click to display all checks for a device.



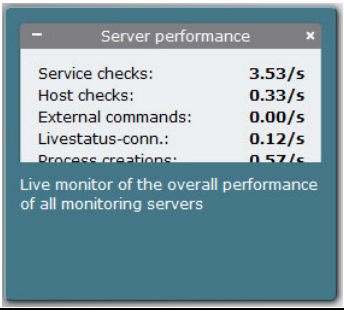
Master control

Global settings can be instantly switched on or off here.



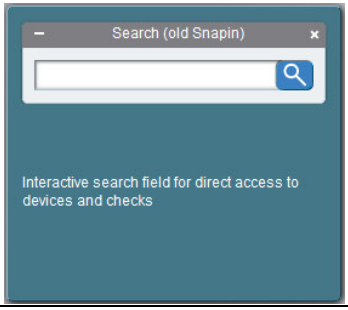
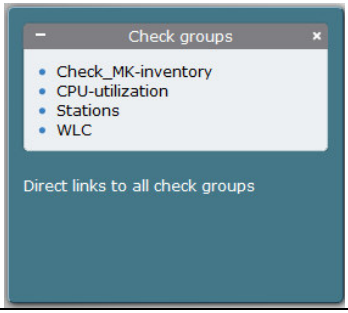
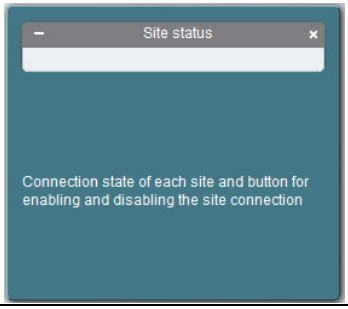
Event console performance

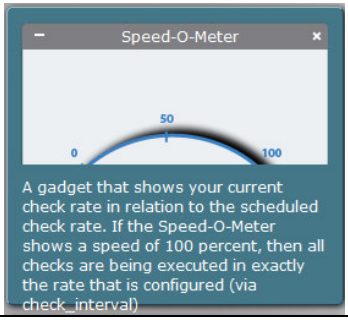
Displays the current performance of the event console, e.g. messages received per second.



Server performance

Shows a current overview of the performance, e.g. how many checks are performed per unit time.

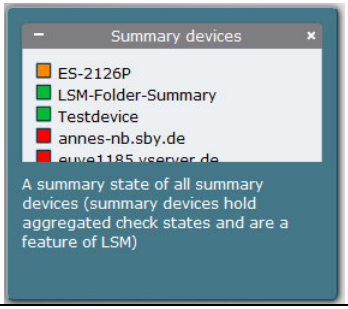
	**Problem devices** Lists all devices where a problem (Down, Warning) has occurred. The colored itemization symbol denotes the status. Click to display all checks for a device.
	**Search (old snap-in)** You can only use this item to search for devices or checks. The search does not include WLAN stations, VPN tunnels, MAC or IP addresses, but it does offer an interactive search function. Please refer to section "Search (old snap-in)" for more information.
	**Check groups** Lists all check groups. Click to display all checks in detail.
	**Site status** Displays the connection status of the different sites and also provides the option to change the status.



Speed-O-Meter

Shows the current check rate as a percentage.

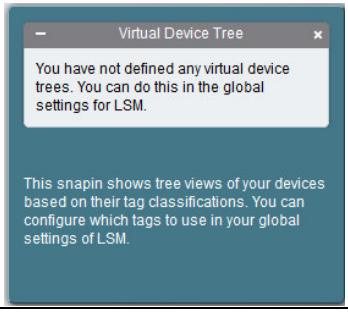
The tool tip shows the values of the current check rates (scheduled, running) and the exact percentage.



Summary devices

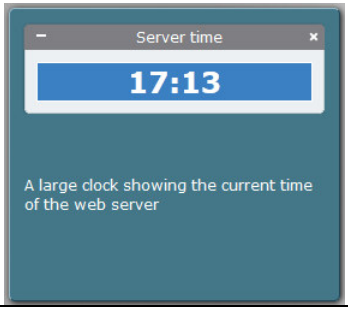
Lists all devices and summarizes the device status in colored bullets.

Click to display all checks for a device.



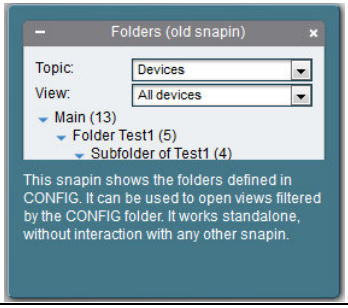
Virtual device tree

Devices can be displayed here in a virtual device tree.



Server time

Shows the server's current time.



File/folder (old snap-in)

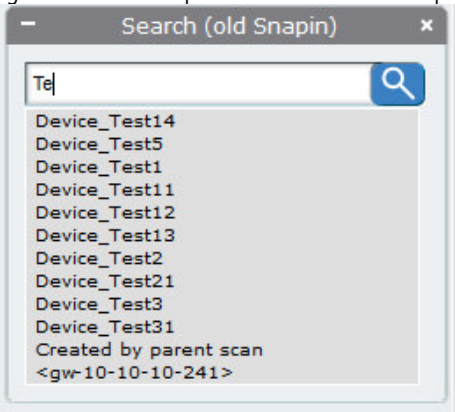
Select the view to be displayed from a drop-down list and the folder where this view is to be displayed.

Search (old snap-in)

This snap-in has been replaced. But since it offers interactive auto-completion, this remains one of the additional snap-ins.

How to search for devices

10. Enter one or more characters from the device name (e.g. test). A drop-down list of all devices containing the character sequence in their name is displayed.



11. Select the preferred device from the list.
12. The view “Checks of device….” then appears in the main window.

How to search for checks

13. Enter one or more characters from the check name.
14. Click the Search icon  .
15. The view “Search checks….” then appears in the main window with all checks that contain the same character sequence.

► Enter a letter sequence that is contained in one or several device names and then click "Search", all checks for this device are displayed, sorted by device name.

8 LANCOM WLAN devices

The LANCOM Large Scale Monitor makes it possible for LANCOM access points (APs) to record details about the WLAN stations (clients) connected them, e.g. Windows notebooks or smartphones. It is also possible to trace the movement of the clients between the various access points (roaming).

8.1 Views

Under the heading "WLAN + VPN" you will find the views "WLAN stations (all states)" and "WLAN stations (connected)". The WLAN stations known to the access points are displayed here.

- WLAN stations (all states)

  All stations known to the access points are listed, i.e. not only those stations that are currently connected with the access point (status "connected") but also any WLAN station that ever logged on to this access point (status "authenticated") Entries can be deleted by highlighting them and selecting "Cleanup" under "Commands". Entries are removed after confirmation.

- WLAN stations (connected)

  All WLAN stations currently associated with the access point are displayed (status "connected").

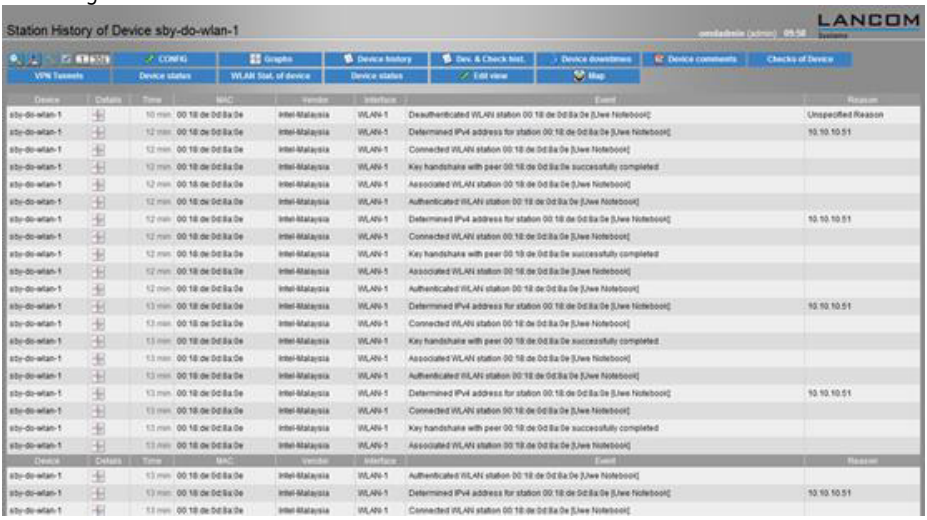
The display shows the device (access point), the MAC address, the vendor of this MAC address and, where available, the IP address and identification of this WLAN station (client).

8.2 Tracking a WLAN station (client)

A mobile WLAN station will log on to different access points as it moves, for example, within a building. As a result, the temporal and local sequence of this movement, known as roaming, can be traced.

By clicking on the MAC address of a WLAN station, the access points that it is associated with are displayed in chronological order.

Alternatively, clicking on the device name shows which clients logged in to this access point in chronological order.



8.2.1 Details on the individual access points

Click the device name to show details on these access points such as information on bands and channels used, history of transfer rates, number of users logged in, etc.

8.3 Maps and floorplans

The spatial distribution of the devices can be represented on a floor plan or map. A map or floor plan must be imported to the relevant folders. If a map is available in the folder of a device or access point, the access point can be displayed on it by using the "Map" button. Please refer to section 5.5.12 "Uploading mapsUploading maps" and section 5.5.13 "Edit map" for further information.

9 LANCOM Large Scale Monitor Mobile

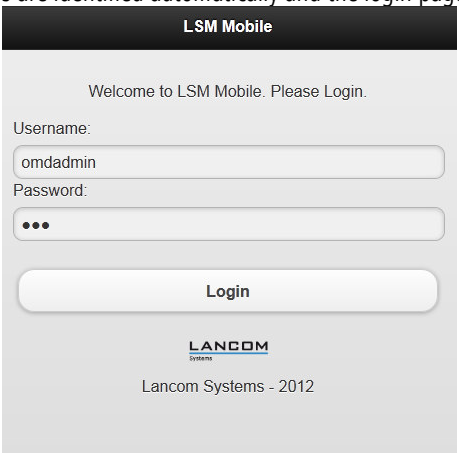
The Large Scale Monitor has a special smartphone interface that gives administrators who are on the move an overview of the monitored devices. Of course only a subsection of the full functionality of the Large Scale Monitor is available for mobile devices, given the restricted screen size of smartphones and the limitations of mobile working. The two widely used platforms Android™ and iPhone™ are supported.

How to invoke the Large Scale Monitor from a smartphone

16. On your smartphone (Android™ or iPhone™), open the browser and enter the URL of the Large Scale Monitor:

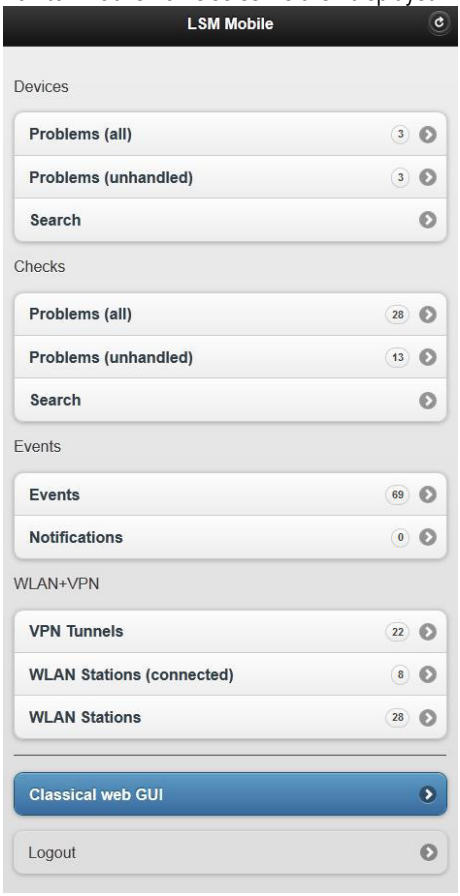
    `https://<LSM-Server>/lsm`

    Mobiles browsers are identified automatically and the login page is displayed.



► The images presented here mostly show the full user interface. Smartphones often display only a part of this, meaning that the rest must be viewed by scrolling through the image.

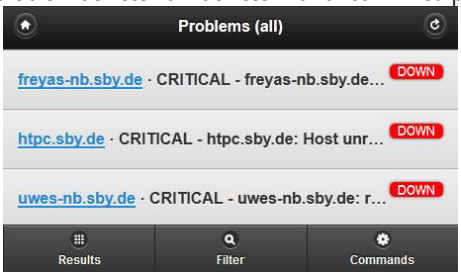
Logon with the usual user name (default: "omdadmin") and password (default: "omd"). The Large Scale Monitor Mobile home screen is then displayed.



► If the mobile browser is not recognized after logging in, it is also to access the Large Scale Monitor Mobile by appending "?mobile=1" to the URL, e.g. https://<LSM-Server>/lsm/check_mk/?mobile=1.

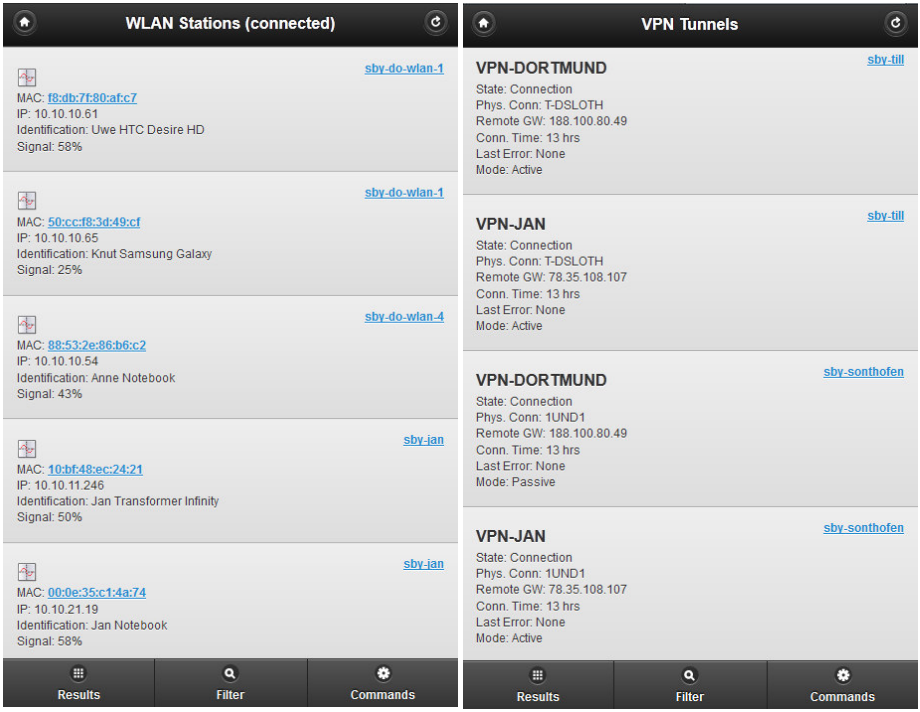
9.1 Working with the Mobile user interface

Within the four areas “Devices”, “Checks”, “Events” and “WLAN+VPN” it is possible to display lists of devices, e.g. "all problem devices" or "devices with unconfirmed problems".



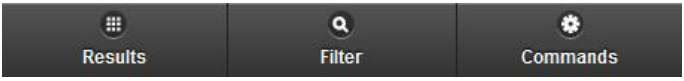
The same applies to checks, events and notifications.

The same applies also to WLAN stations and VPN tunnels.



All views have a “Home”  button at the top left and “Reload”  at the top right of each view. These return the user to the main overview or refresh the current view, respectively.

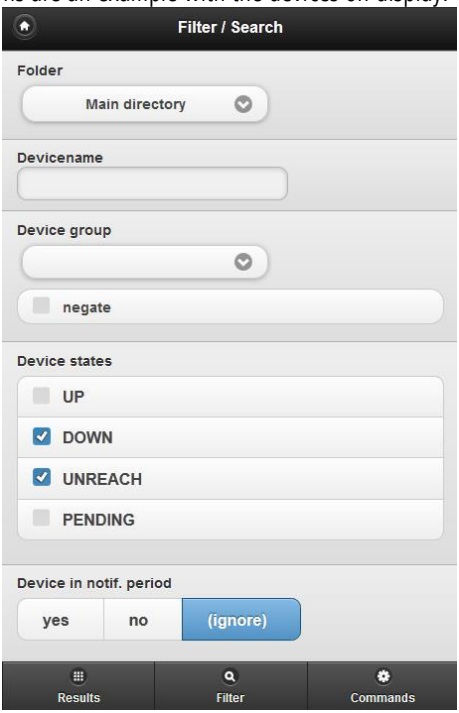
“Result”, “Filter” and “Commands” buttons are located at the bottom of the screen.



9.1.1 Filtering the views

The "Filter" page gives you more detailed filtering for the selected view. The choice of available filter settings depends on the current view. Please refer to section 6.6.2 "Filters" for more information.

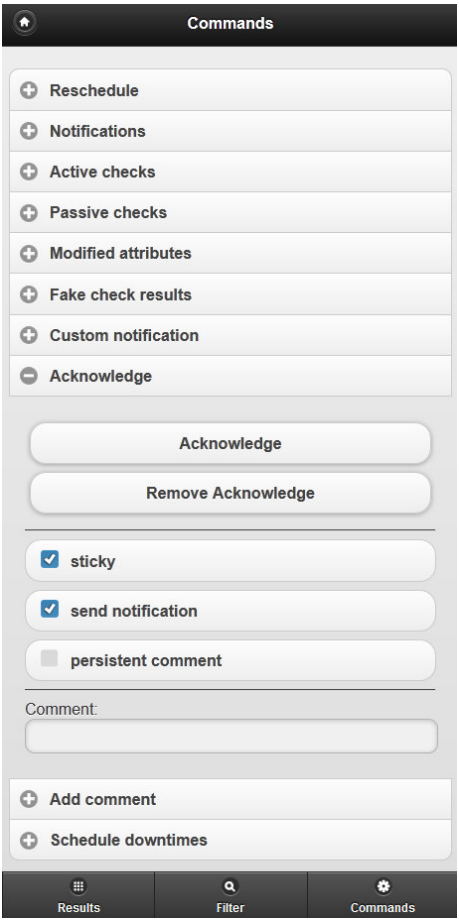
The following filter options are an example with the devices on display.



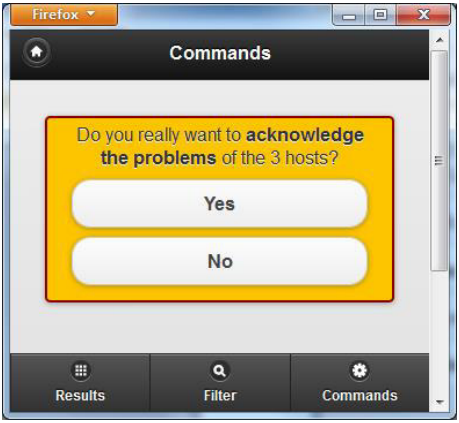
After you have set the filters accordingly, click “Results” to generate the filtered list.

9.1.2 Executing commands

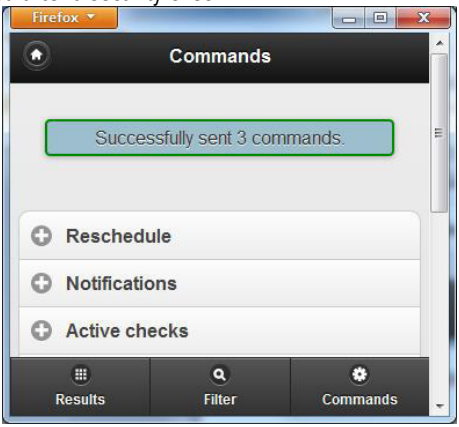
"Commands" can be executed here. In principal these apply to all devices or checks that were displayed previously. If you do not want the command to operate on all of the devices, checks or WLAN stations on display, then apply a filter to the list first. An example of a command for devices is "Acknowledge".



Use the "Acknowledge" feature to confirm the existence a problem after you have entered of a comment.



The command is executed after a security check.



10 Well worth knowing

This section is a collection of further general information, which is loosely related to the LANCOM Large Scale Monitor software.

10.1 Regular expressions – user guide

► The following text is mainly sourced from the Zytrax website (http://www.zytrax.com/tech/web/regex.htm). It has been adapted and summarized.

A regular expression is the term used to describe a codified method of complex searching. They were defined by the American mathematician Stephen Kleene.

The syntax described on this page is compliant with extended regular expressions (EREs) defined in IEEE POSIX 1003.2 (Section 2.8). EREs are now commonly supported by Apache applications or by programming languages such as PHP4, PERL and Javascript. MS Visual Studio, MS Frontpage and many visual editors such as vi, Emac and the GNU-Linux family of tools also support EREs. Extended regular expressions (EREs) are essentially a subset of Basic Regular Expressions (BREs).

10.1.1 Some definitions to start with

We will use the terms literal, metacharacter, target string, escape sequence and search expression in this overview. Here is a definition of these terms:

Literal	A literal is any character used in a search or matching expression. If you are searching for ind in Windows, the ind is a literal string – each character plays a part in the search, it is literally the string we want to find.
Metacharacter	A metacharacter is one or more special characters that have a unique meaning and are not used as literals. For example the character ^ (circumflex or caret) is a metacharacter.
Target string	This term describes the string that is being searched i.e. the string in which we want to find our match or search pattern.
Search expression	This term describes the expression that we use to search the target string.
Escape sequence	An escape sequence is a way of indicating that we want to use a metacharacter as a literal. The escape sequence begins with the metacharacter \ (backslash) and then the metacharacter that we want to use as a literal. For example if we want to find (s) in the target string window(s), then we use the search expression \(s\). If we want to find \\file in the target string c:\\file then we would need to use the search expression \\\\file. Each \ that we want to search for as a literal (there are 2 in \\file) is preceded by an escape sequence \.

10.1.2 The example target strings

In this manual the following target strings are used:
STRING1: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT; DigExt)
STRING2: Mozilla/4.75 [en](X11;U;Linux2.2.16-22 i586)
These are browser string IDs and appear as the Apache variable HTTP_USER_AGENT.

10.1.3 Simple matching

The following are simple examples for search terms and target strings:

Search for	In		Reason
m	STRING1	match	Finds the m in compatible
	STRING2	no match	There is no lowercase m in this string. The search is case sensitive.
a/4	STRING1	match	Found in Mozilla/4.0 – any combination of characters can be used for the match
	STRING2	match	Found in same place as STRING1
5 [	STRING1	no match	The search is looking for a pattern of '5 [' and this does not exist in STRING1. Spaces are valid in searches.
	STRING2	match	Found in Mozilla/4.75 [en]
in	STRING1	match	Found in Windows
	STRING2	match	Found in Linux
le	STRING1	match	Found in compatible
	STRING2	no match	There is an l and an e in this string but they are not adjacent.

10.1.4 Brackets, ranges and negation

Bracket expressions introduce metacharacters, in this case the square brackets allow us to define a list of items to test rather than individual characters. These lists can be grouped into what are known as Character Classes or Groups such as "All digits" for example.

Metacharacter	Meaning
[ ]	Match anything inside the square brackets for one character position once and only once, for example, [12] means match the target to 1 and if that does not match then match the target to 2. If the target string contains neither a 1 nor a 2 then there is no match. [0123456789] means that a match with any digit is possible.
-	The - (dash) inside square brackets is the range separator and allows us to define a range, for example [0123456789] could be rewritten as [0-9]. You can define more than one range inside a list, for example, [0-9A-C] means search for 0 to 9 and A to C (but not a to c). Note: To test for the dash it must be the first or last character inside the brackets that is, [-0-9] will test for - and the digits 0 to 9.
^	The ^ (circumflex or caret) inside square brackets negates the expression, for example, [^Ff] means anything that matches except upper or lower case F and [^a-z] means everything matches except lower case a to z Note: Inserting or removing spaces in the range delimiter values affects the search results.

Now we should try using these metacharacters in the target strings:

Search for	In		Reason
in[du]	STRING1	match	Finds ind in Windows
	STRING2	match	Finds inu in Linux
x[0-9A-Z]	STRING1	no match	The search is again case sensitive, so it does not match the Xt in DigEXt. For a match we would need to use [0-9a-z] or [0-9A-Zt]
	STRING2	match	Finds x2 in Linux2
[^A-M] in	STRING1	match	Finds Win in Windows
	STRING2	no match	The range A to M was excluded in our search so Linux is not found but linux (if it were present) would be found.

10.1.5 Positioning (or anchors)

It is possible to control where in our target strings the matches are valid. The following is a list of metacharacters that affect the position of the search:

Metacharacter	Meaning
^	The ^ (circumflex or caret) outside square brackets means search only at the beginning of the target string, for example, ^Win will not find Windows in STRING1 but ^Moz will find Mozilla.
$	The $ (dollar) means search only at the end of the target string, for example, fox$ will find a match in 'silver fox' since it appears at the end of the string. However, no match is found in the target string 'the fox jumped over the moon'.
.	The space character. (Blank space) means any character in this position, but there must be a character there, e.g. ton. will match with tons, tone and tonneau but not with wanton because there is no character following the “n”.

Note: Many systems and utilities, but not all, support special positioning macros:

- \< match at beginning of word
- \> match at end of word
- \b match at the beginning OR end of word
- \B except at the beginning or end of a word.

Search for	In		Reason
[a-Z]\)$	STRING1	match	Finds t) in DigiExt) Note: The \ is an escape character and is required to treat the) as a literal.
	STRING2	no match	We have a numeric value at the end of this string but we would need [0-9a-z]) to find it.
.in	STRING1	match	Finds Win in Windows.
	STRING2	match	Finds Lin in Linux

10.1.6 Iteration metacharacters

In the following we explain a series of iteration metacharacters (also: quantifiers) that specify the number of occurrences of a character or character string that are required to be found in the search.

Metacharacter	Meaning
?	The ? (question mark) matches the preceding character 0 or 1 time only, for example, colou?r will find both color (0 times u) and color (1 time u).
*	The * (asterisk) matches the preceding character 0 or more times, for example, tre* will find tree (2 times e) and tread (1 time e) and trough (0 times e).
+	The + (plus sign) matches the previous character 1 or more times, for example, tre+ will find tree (2 times e) and tread (1 time e) but NOT trough (0 times e).
{n}	Matches the preceding character, or character range, n times exactly, for example, to find a local phone number we could use . [0-9]{3}-[0-9]{4} which would find any number of the form 123-4567, i.e. 3 digits – 4 digits. Note: The - (dash) in this case, because it is outside the square brackets, is a literal. Values 3 and 4 are enclosed in curly brackets.
{n, m}	Matches the preceding character at least n times but not more than m times, for example, 'Ba{2,3}b' will find 'Baab' and 'Baaab' but NOT 'Bab' or 'Baaaab'. Note: Values 2 and 3 are enclosed in curly brackets.

Let's try these iteration metacharacters now with the sample target strings.

Search for	In		Reason
\(.*l	STRING1	match	Finds the l in compatible Note: The \ is an escape sequence and is required to treat the) as a literal.
	STRING2	no match	Mozilla contains two lls but not preceded by an open parenthesis (no match). Linux has an upper case L (no match).
We had previously defined the above test using the search value l? The search expression l? actually means that all target strings would generate matches, even if they have no l (? Means 0 or 1 times).			
W*in	STRING1	match	Finds Win in Windows.
	STRING2	match	Finds in in Linux preceded by W zero times - so a match.
[xX][0-9a-Z]{2}	STRING1	no match	Finds x in DigExt but only one t.
	STRING2	match	Finds X and 11 in X11.

10.1.7 More "metacharacters"

The following is a set of additional **metacharacters** that provide added power to our searches:

Metacharacter	Meaning
()	The ((open parenthesis) and) (close parenthesis) may be used to group (or bind) parts of our search expression together.
|	The | (vertical bar or pipe) or alternation means find the left-hand OR right-hand values, for example, gr(a|e)y will find 'gray' or 'grey'.

Let's try these metacharacters now with the sample target strings.

Search for			
^([L-Z]in)	STRING1	no match	The '^' is an anchor indicating first position. The search for a match begins at the start of the target string, therefore no match.
	STRING2	no match	Linux does not start the target string so no match.
((4\.[0-3])|(2\.[0-3]))	STRING1	match	Finds the 4.0 in Mozilla/4.0.
	STRING2	match	Finds the 2.2 in Linux 2.2.16-22.
(W|L)in	STRING1	match	Finds Win in Windows.
	STRING2	match	Finds Lin in Linux

11 Glossary: What is ... ?

This section defines some terms to avoid confusion.

11.1 Large Scale Monitor – specific terms

Dashboard

Dashboard refers to an overview comprising of a number of items (dashlets), for example a table, a graph or other visually set-out displays in order to allow quick comprehension of the situation.

There are a number of different pre-configured dashboards. You can also create your own dashboards. Please refer to section 6.9 "Creating and modifying dashboards" for further information.

Device

Device refers to all possible items (routers, switches, access points, printers, servers etc.) within a network. All of these devices can be monitored by the LANCOM Large Scale Monitor.

Multiple devices can be collected into groups of devices (device groups) to simplify the administration and monitoring.

Cluster

Multiple devices of the same type are collected into a cluster (see section 5.5.6 "New cluster").

From an external perspective, these are viewed and treated as a single device of this type. They act as mutual backups if a device should fail.

Check

The LANCOM Large Scale Monitor contacts each device and queries its state and its current parameter values, such as the load or its configuration parameters.

Multiple checks can be collected into groups of checks (Check groups) to simplify the administration and monitoring.

A distinction is made between active and passive checks. The active checks are executed according to the configuration, and these trigger further passive checks.

WLAN station

This documentation summarizes individual and frequently mobile devices, such as laptops or smartphones, under the collective term "WLAN station". A station gains access to the network via an access point. The LANCOM Large Scale Monitor receives the information about the various WLAN stations via the access point.

Where mobile devices are to appear in the device list or search, they need to be imported manually or via CSV file as they cannot normally be accessed via SNMP.

Access point

This is a LANCOM device that is equipped with WLAN capabilities and that provides WLAN stations with access to the network.

View

The data gathered from the Large Scale Monitor can be processed and presented in a variety of ways. A view is a specifically defined representation of devices, checks or parameters.

The default installation package already contains a large number of different views (see section 6.1 "Default views"). Where there are extra requirements, users can customize the way specific data is displayed (see section 6.8 "Editing or creating views").

Structure, folder

Devices and checks are assigned to individual folders. These folders be chosen freely and can, for example, represent the spatial organization (Dortmund, Berlin...) or the organizational structure (Sales, Marketing, Office...) of the company.

Floorplan

The floorplan of a building can be stored as a map to help locate the devices within a building. The devices can be positioned on this map. Please refer to section 5.5.12 "Uploading maps" for further information.

User

A user logs on to the LANCOM Large Scale Monitor by means of a user name and password. Each user can be member of a contact group, which receives notifications about specific events. A user is assigned a role, which determines what rights the user has. Please refer to section 5.12 "User" for further information.

Contact group

A contact group is a collection of multiple users. Notification (by e-mail) is sent to this group should certain events occur. Please refer to section 5.14 "Contact groups" for further information.

Permissions, roles

Every user is assigned one or more roles and the associated rights. There is a difference between:

- Configuration rights

  The right to change the parameters of devices and folders and to create new ones.

- Monitoring rights

  This right can be granted only in addition to the configuration rights. It allows for current state of the devices or folders to be displayed

Administrators have the right to monitor and configure everything.

Please refer to section 5.12 "User" for further information.

Autocheck profile

Using an autocheck profile simplifies the discovery of checks that are available for a device. This method is suitable for installations where a large number of identical or similar devices are monitored, i.e. where a bulk discovery should be avoided due to the high number of devices and the time-consuming discovery.

An autocheck profile is created on the basis of an already installed device. It contains all of the checks that were discovered for this example device. The autocheck profile can then be applied on further devices without the need to carry out the bulk discovery.

For more information about creating and applying autocheck profiles, please refer to section 5.6 "Autocheck profiles".

11.2 Common standards

The following briefly explains some of the common standards that are in use.

SNMP

The Simple Network Management Protocol is a network protocol designed by the IETF to monitor and control network elements (e.g. routers, servers, switches, printers, computers, etc.) from a central station. The protocol regulates the communication between the monitored devices and the monitoring station. SNMP describes the structure of the data packets that can be sent, and the communication sequence. The protocol has been designed so that any network-enabled device can be monitored. The tasks of network management that are possible with SNMP include:

- Monitoring of network components,
- Remote control and remote configuration of network components,
- Error detection and error notification.

Due to its simplicity, modularity and versatility SNMP has become a standard that is supported by the majority of management programs and devices.

VPN

A VPN (Virtual Private Network) represents a closed network that can even be physically connected over a public network such as the Internet. VPN tunnels shield these connections from the outside and are used exclusively for the communications within the VPN itself.

WLAN

Wireless Local Area Network (WLAN) refers to a local radio network. This documentation refers to WLAN as the connectivity medium for mobile devices (notebooks, smartphones) and the fixed access points.

11.2.1 About the radio signals used by WLAN devices

(Frequency) band

The frequency of the WLAN access point.

Tx power

Mean transmission power in dBm

Noise

Signal noise in dBM

Load

Channel load as percentage

Background scan

Rate at which the device is configured to repeat the background scan

Wireless Protected Access (WPA)

Wi-Fi Protected Access (WPA) is an encryption method for wireless networks (wireless LAN). After the Wired Equivalent Privacy (WEP) from the IEEE 802.11 standard proved to be insecure, the Wi-Fi Alliance established a subset of IEEE 802.11i under the name of WPA. The successor to this is WPA2.

Basic Service Set Identifier (BSSID)

The Basic Service Set Identifier, or BSSID for short, is the unique identifier of an access point in a WLAN. The IEEE 802.11-1999 wireless LAN specification defines a BSSID as the MAC address of an access point (AP) in infrastructure mode (BSS). The BSSID thus uniquely identifies each wireless access point, which is important for distinguishing between access points with the same ESSID.

Rx error ratio

Indicates the percentage failure rate of packets received.

Tx error ratio

Indicates the percentage failure rate of packets sent.

Index