WNMS v.1.2

Quick Start Guide

Revision 1.0
June 1, 2012

Contents

About this Guide

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of basic networking concepts and wireless Internet access infrastructures.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

Additional information that may be helpful but which is not required.

Important information that should be observed.

bold	Menu commands, buttons, input fields, links, and configuration keys are displayed in bold
italic	References to sections inside the document are displayed in italic.
`<code>`	File names, directory names, form names, system-generated output, and user typed entries are displayed in constant-width type

Introduction

WNMS is an enterprise grade Wireless Network Management System (WNMS). Single software solution simplifies large number of management and monitoring tasks for network administrator. Comprehensive network management software supports up to several thousand of nodes. Multiple networks may be maintained and monitored using one server. Rich feature set helps to diagnose network problems effectively, visualize network on map, perform automatically scheduled firmware upgrades, track states of devices, get alerts about failures, collect statistics and many other things. Web-based system environment supports multi-user accounts. Several administrators may manage different networks on the same server, without having access to each other's equipment.

The WNMS system architecture allows configuring or performing firmware upgrades on any network infrastructure. Monitored devices can be on LAN behind a NAT or on WAN. Scalable software design is perfectly suited for small and large networks. Rapidly growing networks may be split it into smaller logical groups (smaller networks) and assigned to different administrators. All information about the devices that are monitored (name, MAC, serial number, IP, firmware version) is stored in WNMS server. Information storage in one place, quick search capabilities, data export options simplify the inventory management. Each network device can be monitored individually with defined tracking parameters (standard and custom based on SNMP value). Reported alerts are shown on WNMS dashboard in a real time. Furthermore, system has the ability to notify contacts (via email) when problems arise and are resolved. Alert history is stored on the server allowing analysis of failures that happened in the past.

System Architecture

WNMS systems use Client-Server structure. WNMS agent must be activated on the management interface of each device. This is a special program that runs on the device and communicates with the WNMS server though proprietary XML based protocol. The WNMS agent listens and executes commands from the WNMS server and returns required data.

WNMS server consists of the following components:

- Data collector
- Database
- Monitor daemon
- Graphical user interface

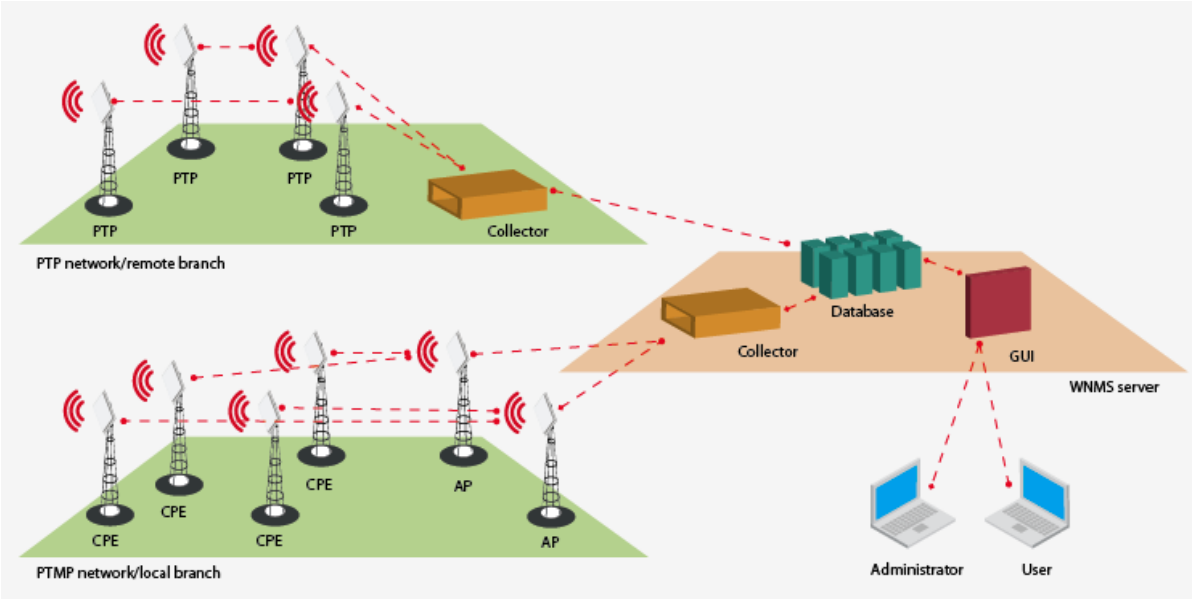


Figure 1 – WNMS Architecture

Data collector is an intermediate point between WNMS agent and a database. Each agent in defined time interval sends heartbeats (special packages with information) to the collector. All information (statistics, alerts, etc) is transferred via heartbeat. Collector extracts information from heartbeat, processes it and stores data in the database. The collector also sends reply heartbeats to the devices if there are any assigned tasks for the particular device (e.g. get troubleshoot file, upgrade firmware, etc). The WNMS server contains modular architecture, therefore several collectors may exist. If the link between database and collector is lost, all the information will be stored locally on the collector server and will be transferred to the database as soon as the link is up again.

Database is at the heart of the WNMS system. It stores all information about devices, networks and their configurations, also keeps alerts and statistical data. Collectors, monitor daemon and GUI communicate directly with the database.

Monitor daemon is a special program that runs on WNMS server and is responsible for device availability alert (device is online/offline). In addition, this process is responsible for sending e-mail notifications to the predefined contacts.

Graphical user interface is a face of the system. All network management tasks are done via WEB-based GUI.

System Requirements

In order to install WNMS software the system must match following requirements:

WNMS server

- Operating system:
  - Ubuntu 9.10 or later
  - Debian 6.0 ("squeeze")
  - Windows (Windows XP, Windows Server 2003, Windows VISTA, Windows Server 2008 and Windows 7)
- Minimum hardware requirement (for the network with several hundreds of devices)
  - 1 GHz x86 processor
  - 1.5 GB of RAM
  - 20 GB of hard-drive space
  - Network/Internet access
- Recommended hardware requirement (for the network with several thousands of devices)
  - 2 GHz x86 processor
  - 4 GB of RAM
  - 50 GB of hard-drive (depending on a history data keeping)
  - Network/Internet access

Client

- For WNMS management the administrator's computer must have Adobe Flash Player version 9.0.28 or later installed.
- Internet Explorer v7.0 or higher
- Mozilla Firefox v3.5 or higher

Communication between Devices and WNMS Server

WNMS server listens for the devices by default on HTTP (TCP 80) port although can be configured for a communication through HTTPS. This is only one requirement for a firewall. In such way devices can be controlled via NAT from WNMS.

WNMS Installation

WNMS Installation on Windows OS

This section provides instructions on how to install and uninstall WNMS on Windows OS (Windows XP, Windows Server 2003, Windows VISTA, Windows Server 2008 and Windows 7).

Installation Steps

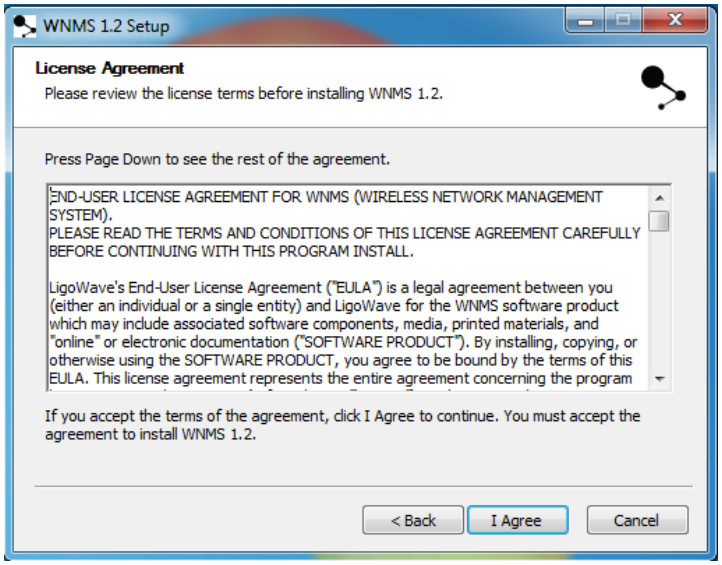
WNMS requires HTTP 80 port, therefore it is recommended to close all the programs before installation, because some of the programs may use TCP ports required for proper WNMS operation (for example, HTTP (80) port can be occupied by Skype).

Follow these steps to download and install WNMS server on Windows OS.

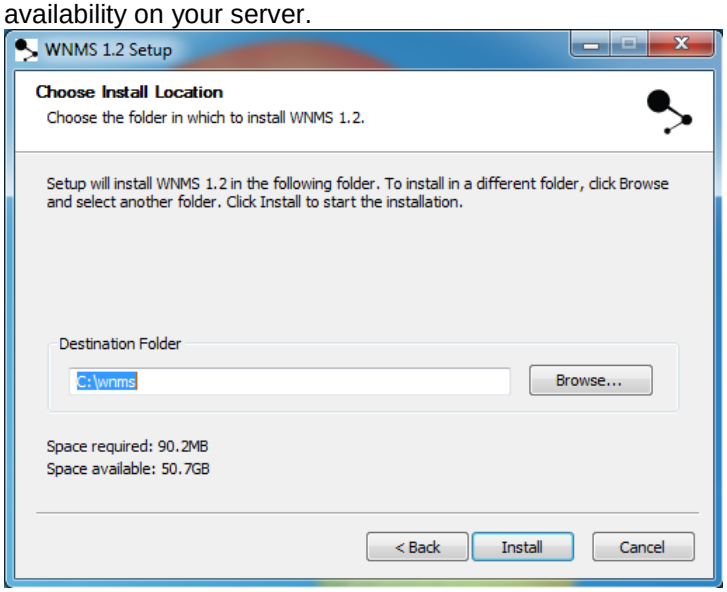
Step 1. Download WNMS installer for windows from www.ligowave.com or www.deliberant.com under WNMS section.

Step 2. Run the executable installer and follow the instructions provided by the installation wizard. It is strongly recommended that you close all other running programs before continue.

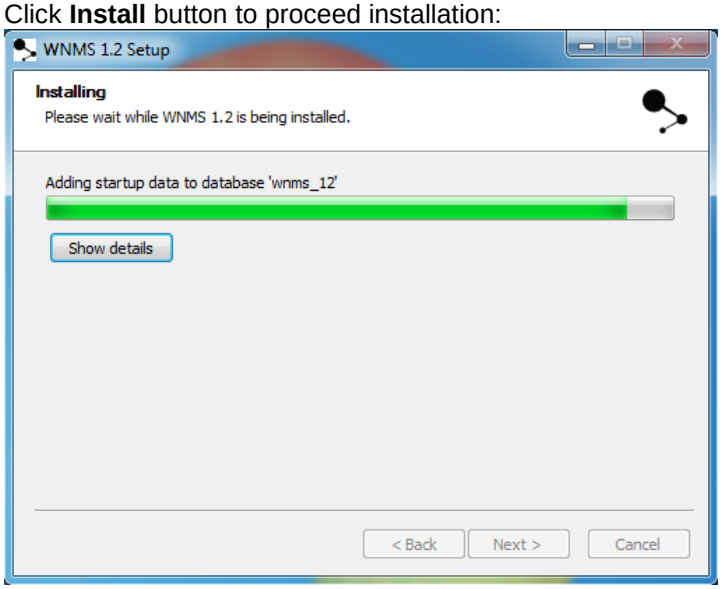
Step 3. The **License Agreement** window will appear. Please read carefully and select **I Agree** to continue.



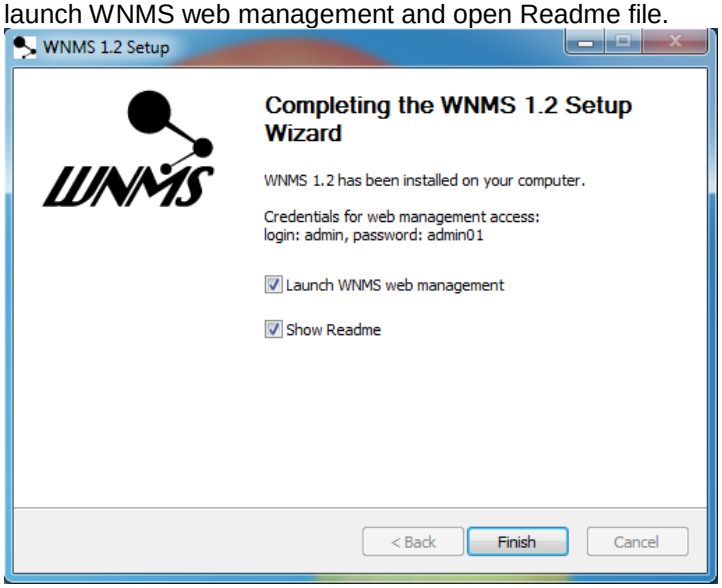
Step 4. **Choose install location** window offers to install the WNMS server in the default location `C:\wnms`, or click **Browse...** to specify different path. The installer will check free space availability on your server.



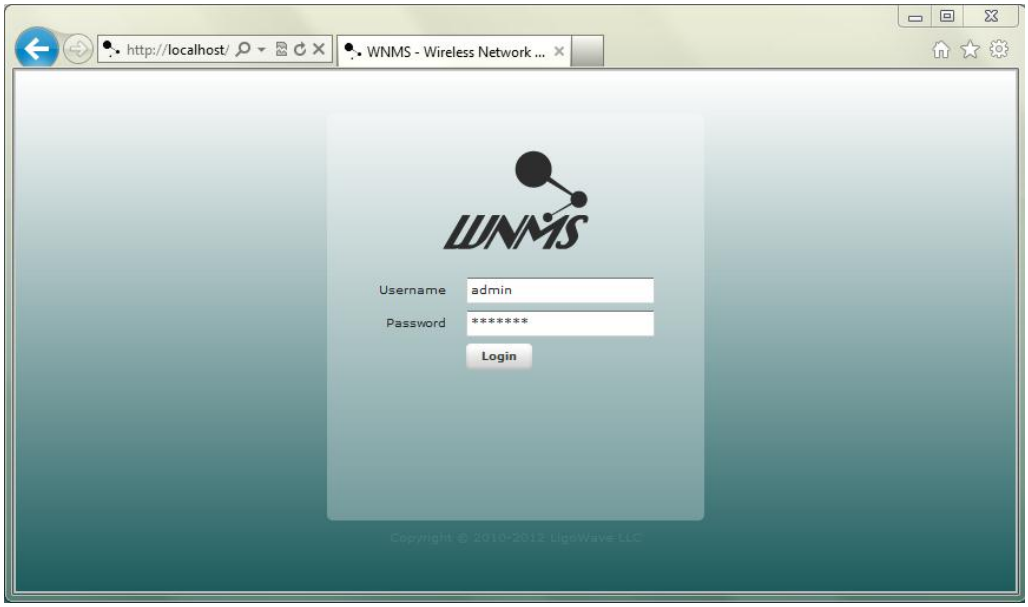
Step 5. Click **Install** button to proceed installation:



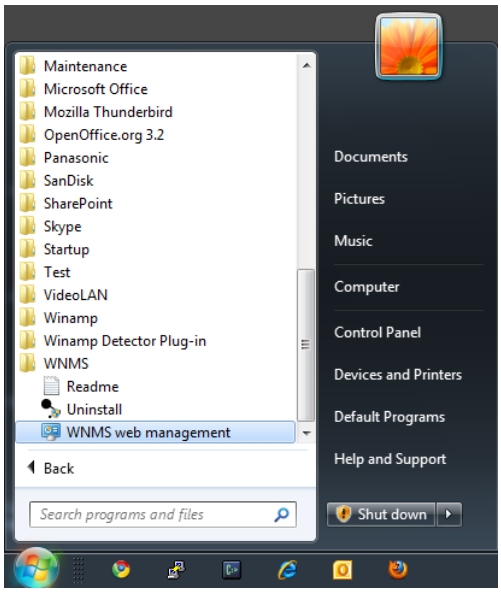
Step 6. After the WNMS server was successfully installed, the welcome window offers you to launch WNMS web management and open Readme file.



Step 7. Login in to the WNMS server web management interface. Default login credentials are: **admin/admin01**.



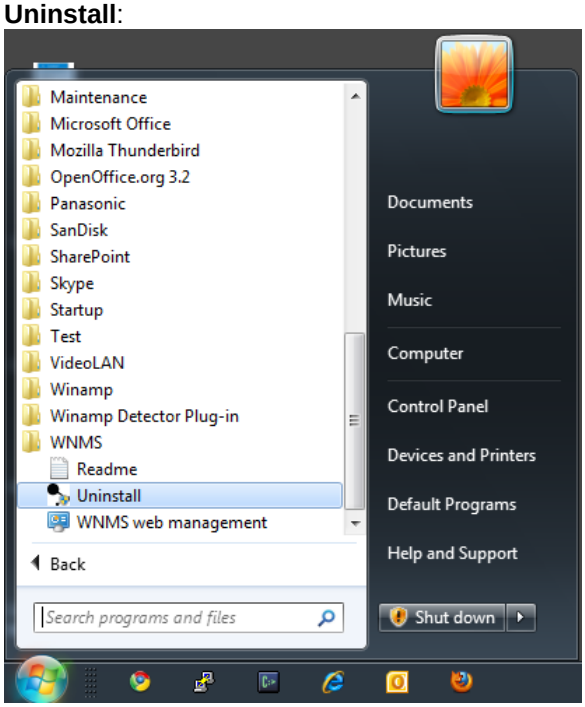
Step 8. To launch the WNMS server on browser, click **Start** → **Programs** → **WNMS** → **WNMS web management** (or simply specify computers where the WNMS was installed IP address into the browser's address line)



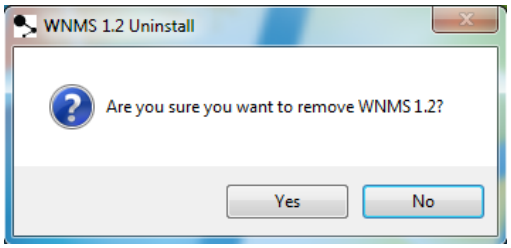
Uninstallation

Follow the steps to remove WNMS server:

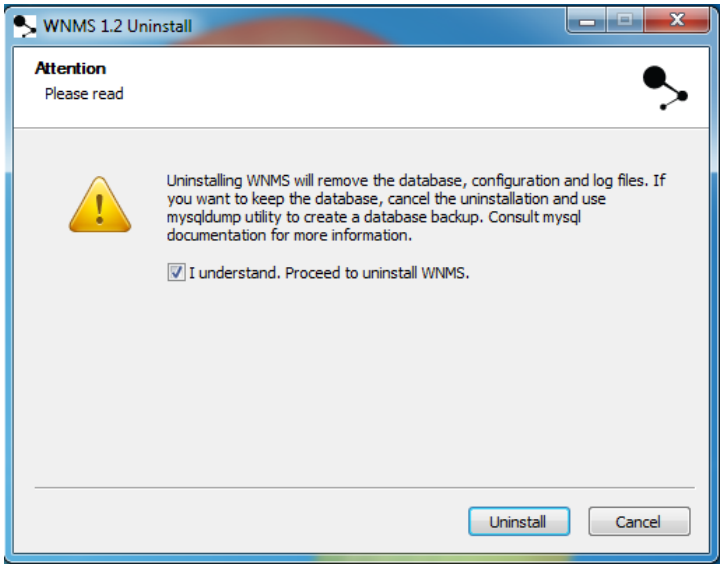
Step 1. To remove WNMS server from the system, select **Start** → **Programs** → **WNMS** → **Uninstall**:



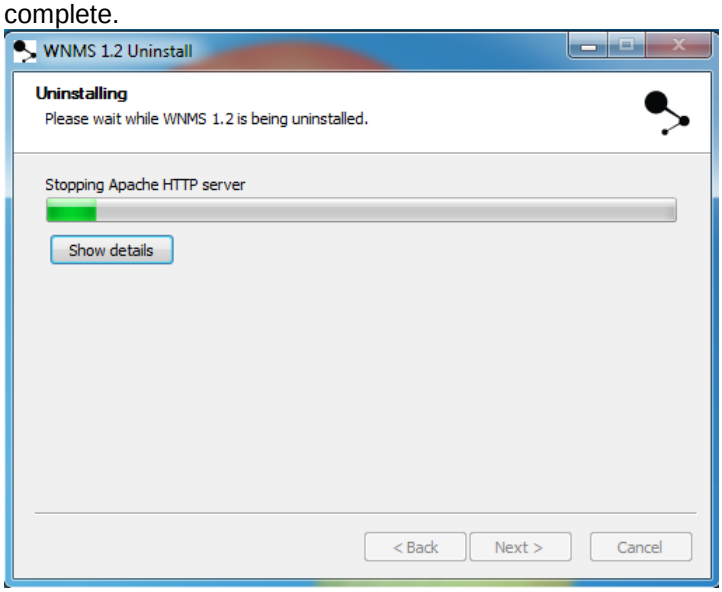
Step 2. Confirm on WNMS uninstallation:



Step 3. Select **Allow to proceed** to begin full unintsallation process:



Step 4. After the uninstallation procedure has been finished successfully, click **Finish** button to complete.



Step 5. The WNMS server has been successfully uninstalled.

WNMS Installation on Linux OS

WNMS requires HTTP 80 port, therefore it is recommended to close all the programs before installation, because some of the programs may use TCP ports required for proper WNMS operation (for example, HTTP (80) port can be occupied by Skype).

This section provides instructions on how to install and uninstall WNMS on Ubuntu 9.10 or later Debian testing (squeeze) OS. The WNMS system is packed into two `*.deb` packages:

- **WNMS server**:
  - Database,
  - Monitor daemon,
  - Graphical user interface
- **WNMS collector:**
  - Data collector

Installation Steps on Command-line Interface

This section describes how to install WNMS system on Ubuntu distribution, assuming that installation on Debian can be done in the same way.

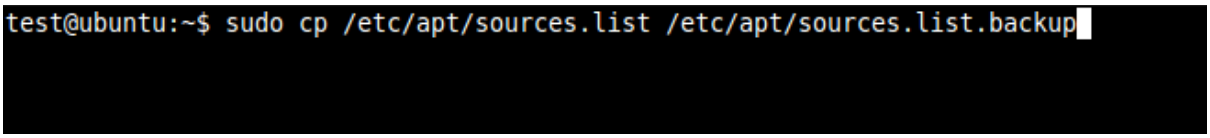
The command-line interface is recommended for installing WNMS because desktop environment is not always available (e.g. Ubuntu server without a desktop environment).

Use **Terminal** program for Ubuntu desktop environment; or a **Konsole** program if Kubuntu desktop environment is used.

Follow the steps to install WNMS server and collector:

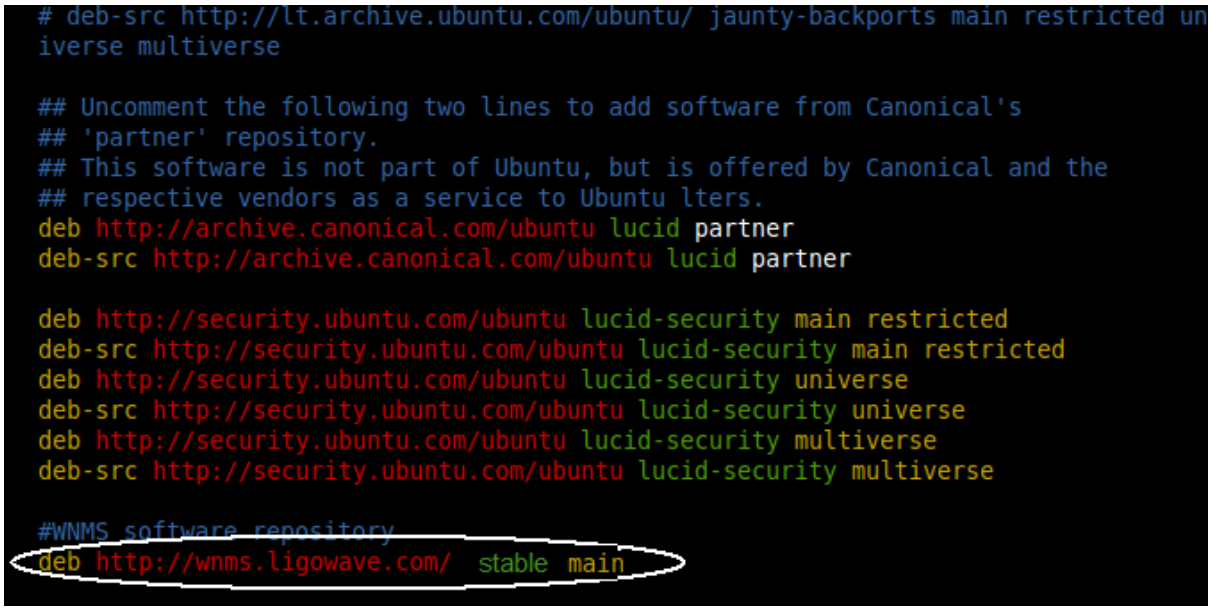
Step 1. **Create a backup file of the repository list**. The following command creates a backup file `sources.list.backup` in the directory `/etc/apt/sources.list`. Type command:

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.backup
```



Step 2. **Add WNMS software repository** using VIM text editor in `sources.list` file:

```
deb http://wnms.ligowave.com/ stable main
```



Step 3. **Update local server package database**. Type command:

```
sudo apt-get update
```

Step 4. **Install WNMS Server.** Type command:

```
sudo apt-get install wnms-server
```

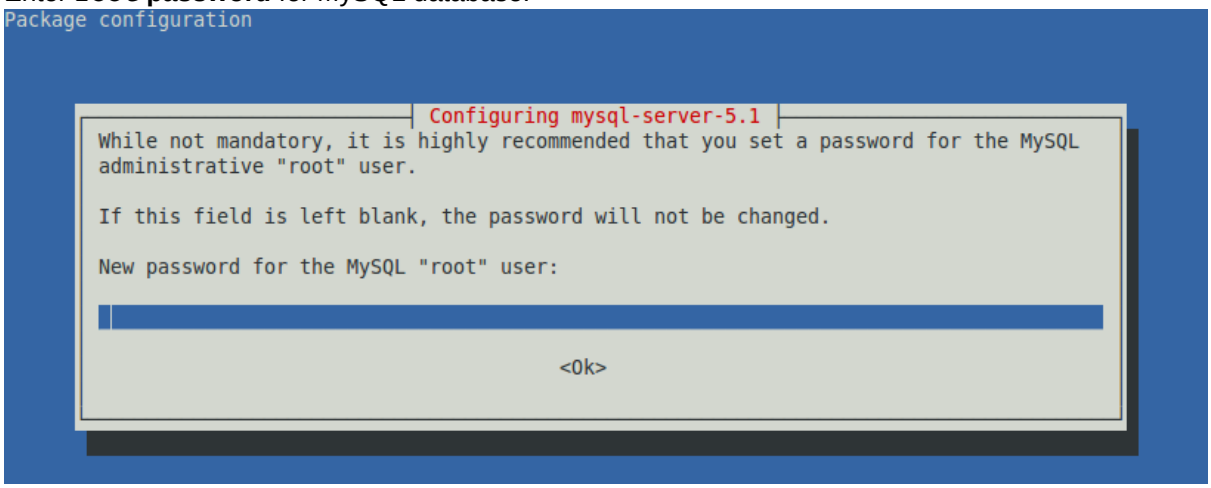
```
test@ubuntu:~$ sudo apt-get install wnms-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common libapache2-mod-php5 libapr1
  libaprutil1 libaprutil1-dbd-mysql libaprutil1-ldap libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libmysqlclient16 libnet-daemon-perl libplrpc-perl mysql-client-5.1
  mysql-client-core-5.1 mysql-common mysql-server-5.1 mysql-server-core-5.1 php5-common php5-mysql
  ssl-cert
Suggested packages:
  apache2-doc apache2-suexec apache2-suexec-custom php-pear dbishell libipc-sharedcache-perl tinyca
  mailx php5-suhosin
The following NEW packages will be installed:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common libapache2-mod-php5 libapr1
  libaprutil1 libaprutil1-dbd-mysql libaprutil1-ldap libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libmysqlclient16 libnet-daemon-perl libplrpc-perl mysql-client-5.1
  mysql-client-core-5.1 mysql-common mysql-server-5.1 mysql-server-core-5.1 php5-common php5-mysql
  ssl-cert wnms-server
0 upgraded, 24 newly installed, 0 to remove and 3 not upgraded.
Need to get 31.4MB of archives.
After this operation, 76.2MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

Type **Y** (yes) to confirm installation:

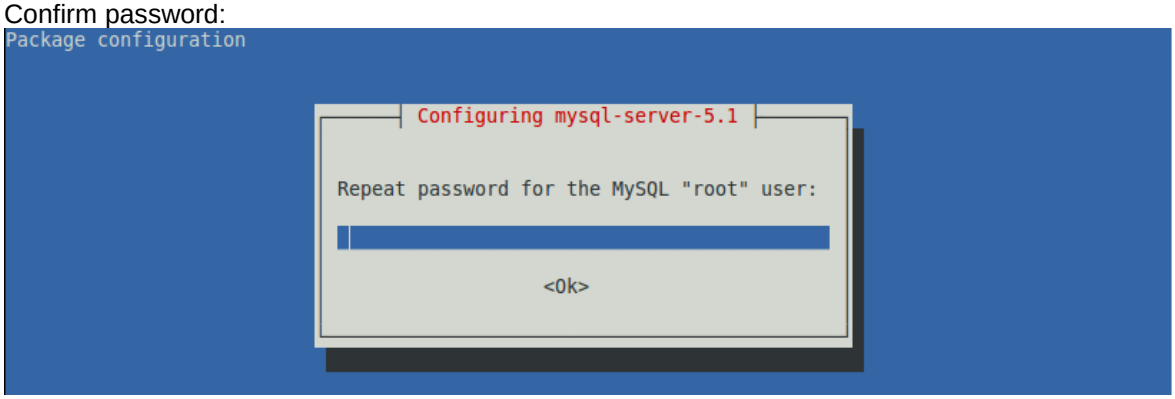
```
test@ubuntu:~$ sudo apt-get install wnms-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common libapache2-mod-php5 libapr1
  libaprutil1 libaprutil1-dbd-mysql libaprutil1-ldap libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libmysqlclient16 libnet-daemon-perl libplrpc-perl mysql-client-5.1
  mysql-client-core-5.1 mysql-common mysql-server-5.1 mysql-server-core-5.1 php5-common php5-mysql
  ssl-cert
Suggested packages:
  apache2-doc apache2-suexec apache2-suexec-custom php-pear dbishell libipc-sharedcache-perl tinyca
  mailx php5-suhosin
The following NEW packages will be installed:
  apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common libapache2-mod-php5 libapr1
  libaprutil1 libaprutil1-dbd-mysql libaprutil1-ldap libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libmysqlclient16 libnet-daemon-perl libplrpc-perl mysql-client-5.1
  mysql-client-core-5.1 mysql-common mysql-server-5.1 mysql-server-core-5.1 php5-common php5-mysql
  ssl-cert wnms-server
0 upgraded, 24 newly installed, 0 to remove and 3 not upgraded.
Need to get 31.4MB of archives.
After this operation, 76.2MB of additional disk space will be used.
Do you want to continue [Y/n]? y
WARNING: The following packages cannot be authenticated!
  wnms-server
Install these packages without verification [y/N]? y
```

Type **Y** (yes) for install packages without verification.

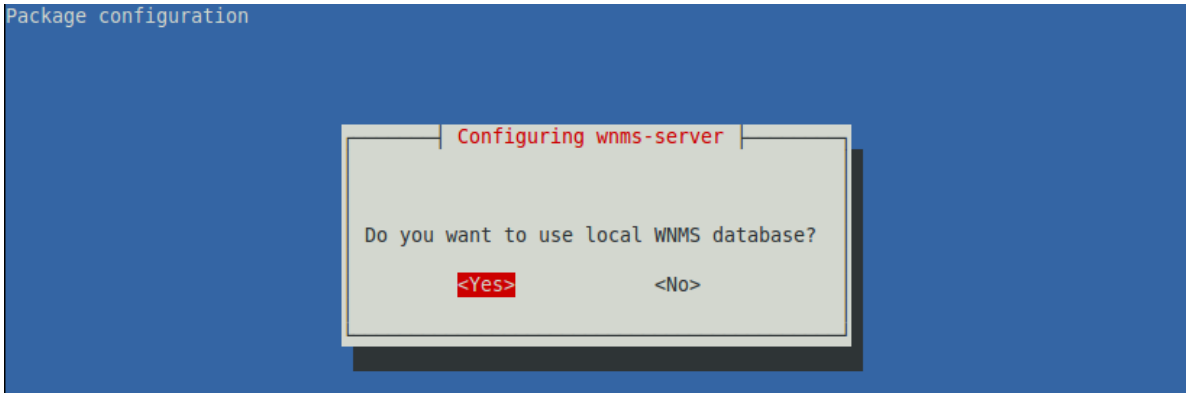
Enter **`root` password** for MySQL database:



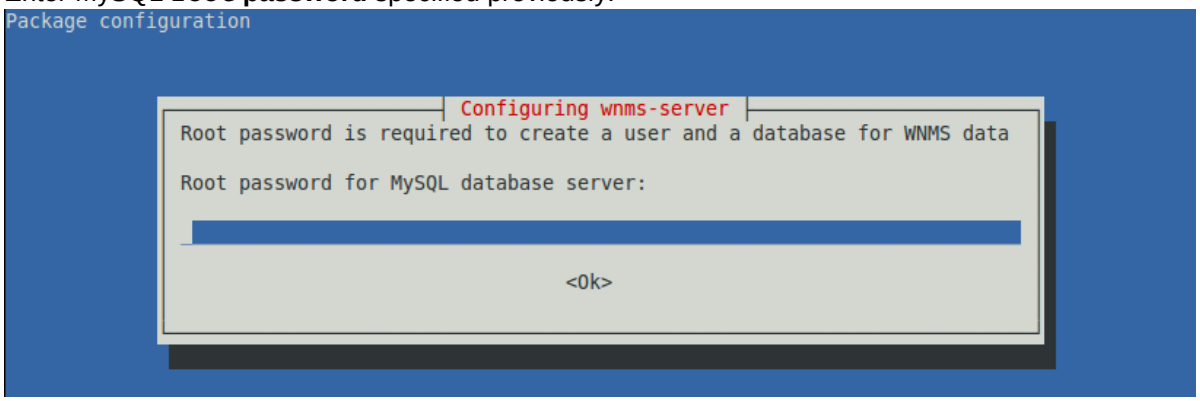
Confirm password:



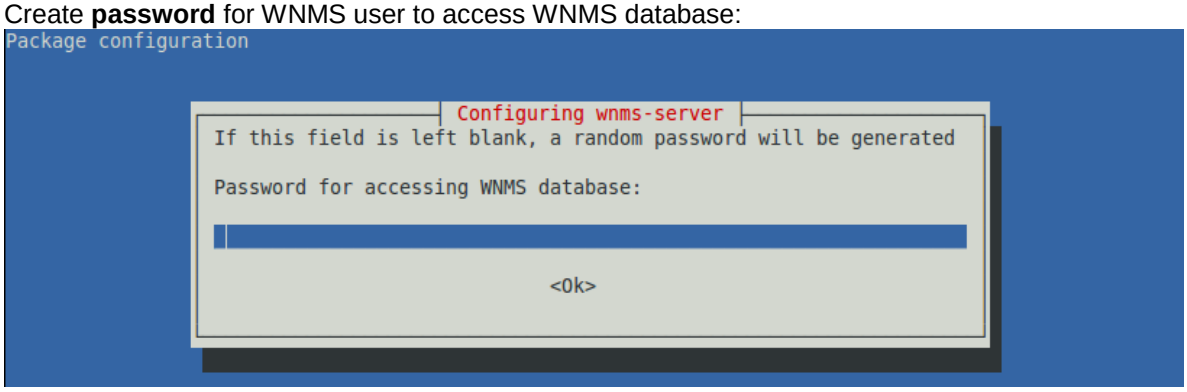
Create local database for WNMS server – choose **Yes**:



Enter MySQL **`root` password** specified previously:



Create **password** for WNMS user to access WNMS database:



Check if all services are installed and started successfully:

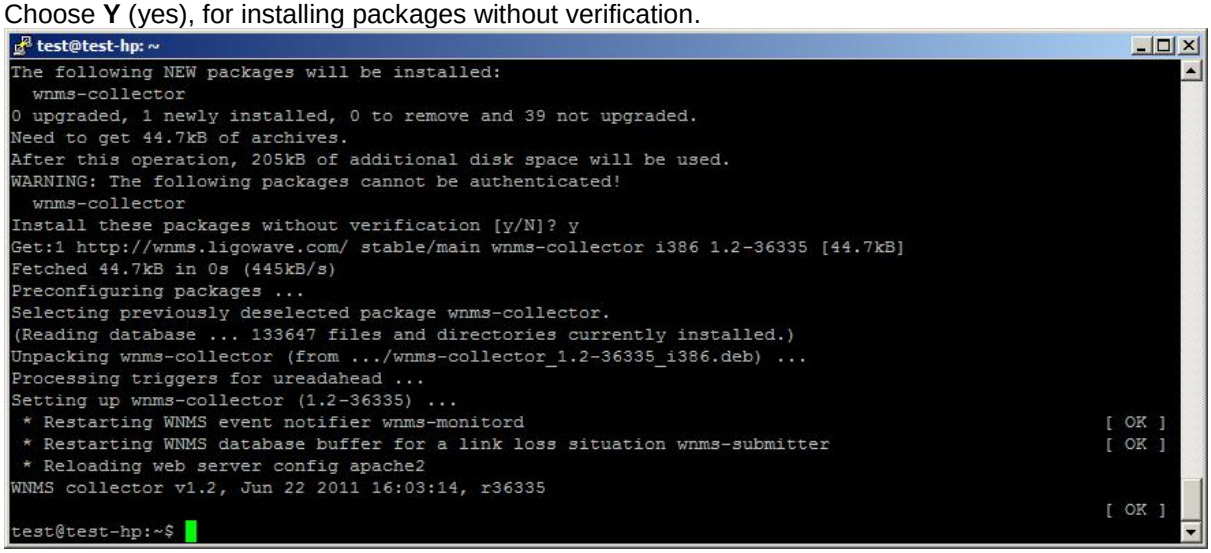
```
Enabling module dir.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module status.
Enabling module auth_basic.
Enabling module deflate.
Enabling module authz_default.
Enabling module authz_user.
Enabling module authz_groupfile.
Enabling module authn_file.
Enabling module authz_host.
Enabling module reqtimeout.

Setting up apache2-mpm-prefork (2.2.14-5ubuntu8.3) ...
 * Starting web server apache2                                          [ OK ]

Setting up php5-common (5.3.2-1ubuntu4.5) ...
Setting up libapache2-mod-php5 (5.3.2-1ubuntu4.5) ...

Creating config file /etc/php5/apache2/php.ini with new version
 * Reloading web server config apache2                                  [ OK ]

Setting up libhtml-template-perl (2.9-1) ...
Setting up php5-mysql (5.3.2-1ubuntu4.5) ...
Setting up ssl-cert (1.0.23ubuntu2) ...

Setting up wnms-server (1.2-30970) ...
 * Restarting WNMS event notifier wnms-monitord                         [ OK ]
 * Reloading web server config apache2                                  [ OK ]

Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
test@ubuntu:~$
```

Step 5. **Install WNMS Collector.** Type command:

```
sudo apt-get install wnms-collector
```

```
test@ubuntu:~$ sudo apt-get install wnms-collector
[sudo] password for tester:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  wnms-collector
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 34.0kB of archives.
After this operation, 176kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  wnms-collector
Install these packages without verification [y/N]? y
```

Choose **Y** (yes), for installing packages without verification.



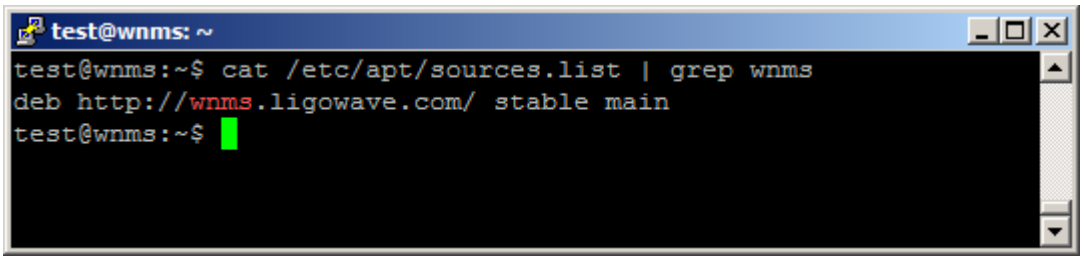
Step 6. Enter the hostname or IP address with ending `/wnms` (e.g. `192.168.2.100/wnms`) on web browser of the WNMS server and the login page of the WNMS will be displayed. Default login credentials are: **admin/admin01**.

The WNMS may be installed using “dpkg” utility. However it is recommended to use apt-get method as it handles all WNMS packages dependencies and installs them automatically.

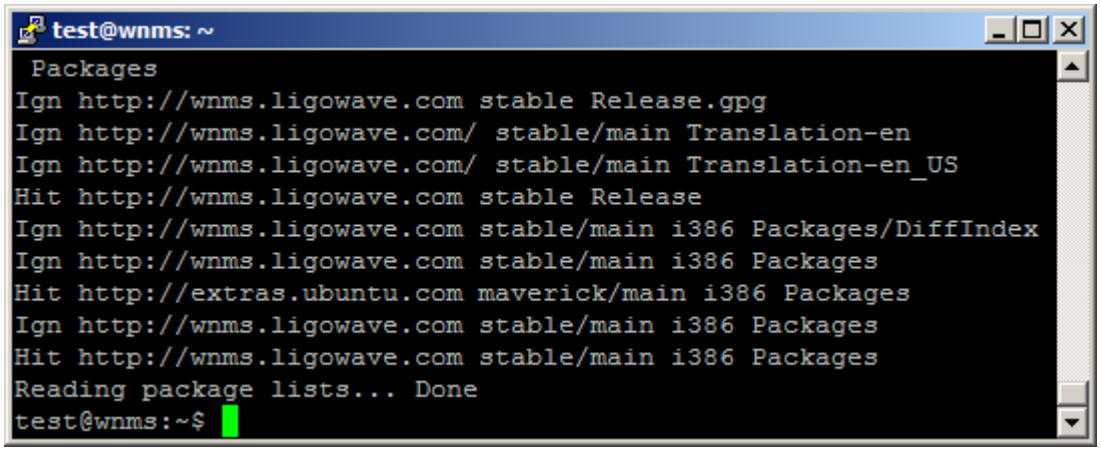
Upgrade from previous version

Step 1. Login to your linux machine through SSH or open console windows on GUI environment

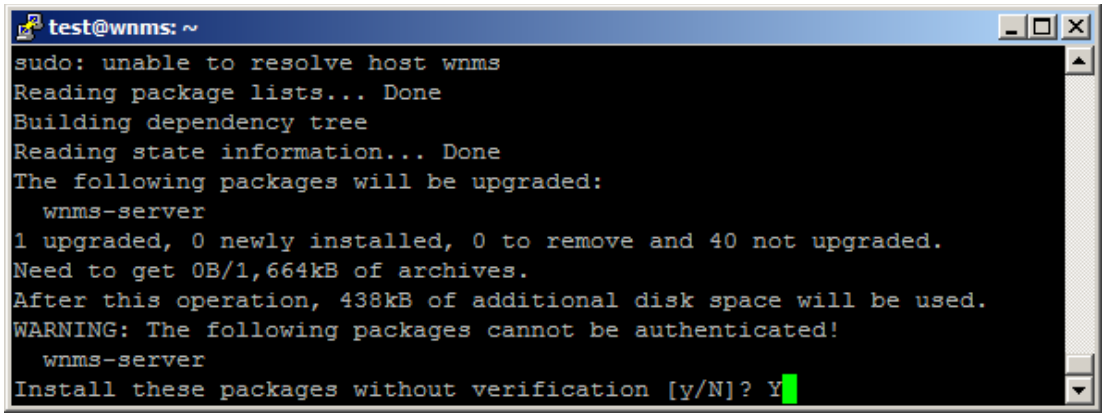
Step 2. Make sure you have valid WNMS repository URL



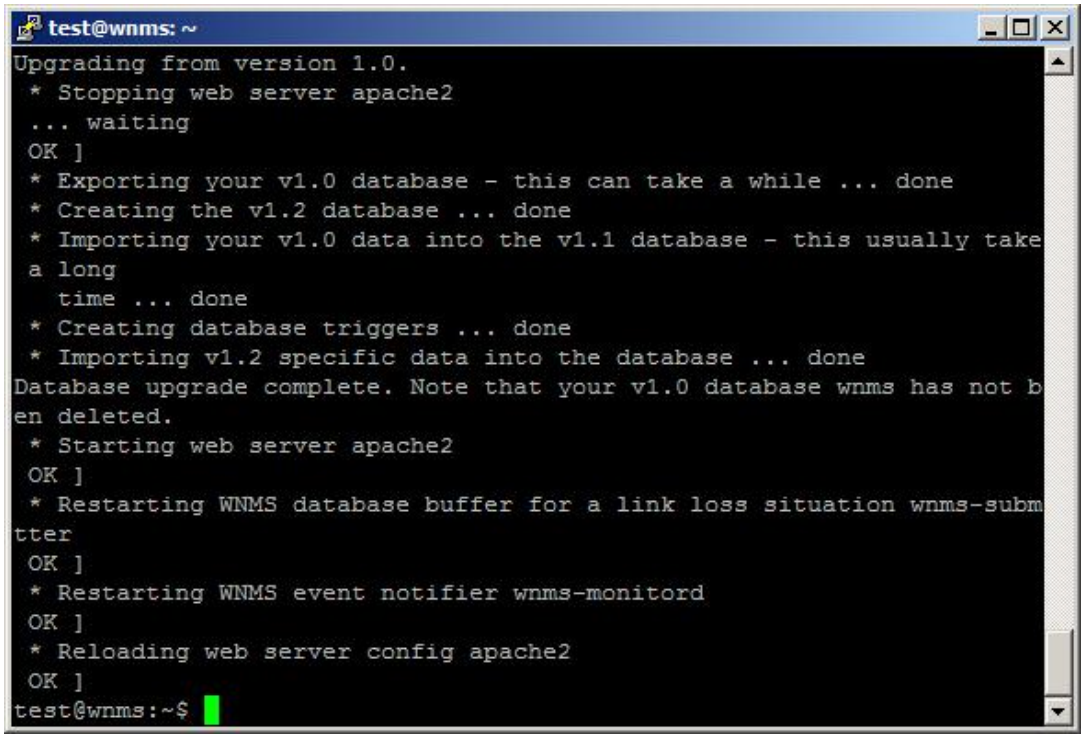
Step 3. Update your repository: sudo apt-get update



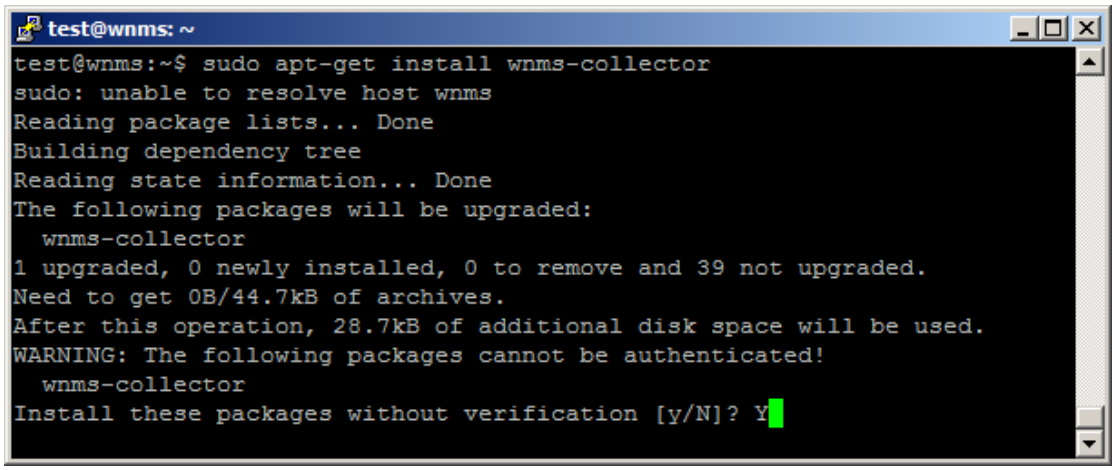
Step 4. Install wnms server: sudo apt-get install wnms-server
Press **Y** and enter

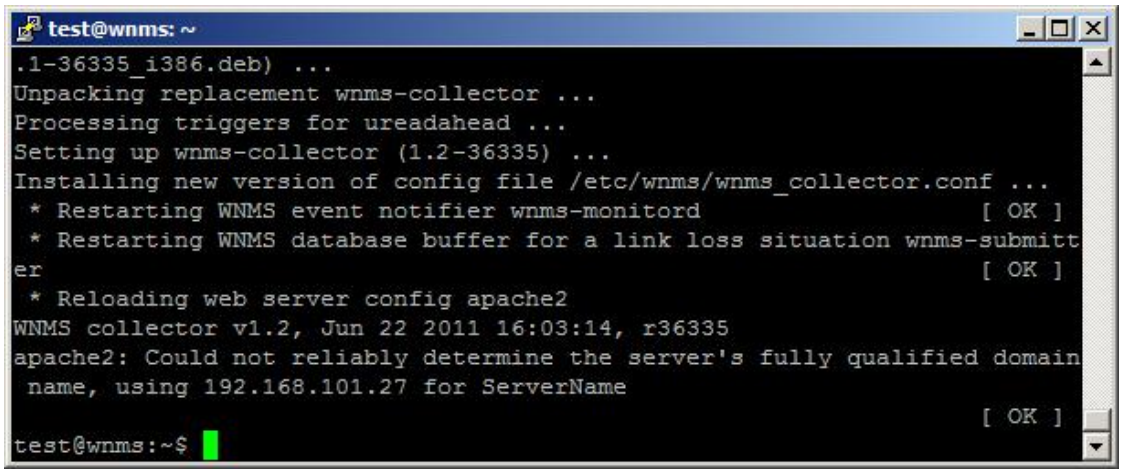


Step 5. Upgrade may take from few to 20 minutes depending on data size on database



Step 6. Install wnms-collector: sudo apt-get install wnms-collector
Press **Y** and enter





Uninstallation

Follow the steps to remove WNMS system from the system:

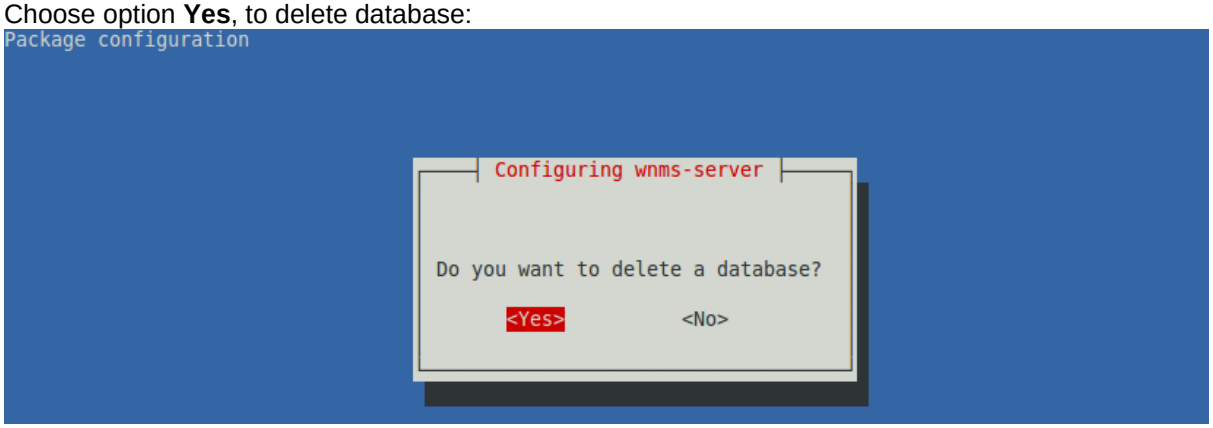
Step 1. **First uninstall WNMS server**. Type command:

```
sudo apt-get purge wnms-server
```

```
test@ubuntu:~$ sudo apt-get purge wnms-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libhtml-template-perl mysql-server-5.1 mysql-server-core-5.1 php5-mysql libapache2-mod-php5 php5-common
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  wnms-server*
0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 2,322kB disk space will be freed.
Do you want to continue [Y/n]? y
```

Type **Y** (yes) to confirm uninstall.

Choose option **Yes**, to delete database:



Finish WNMS server uninstallation:

```
test@ubuntu:~$ sudo apt-get purge wnms-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libhtml-template-perl mysql-server-5.1 mysql-server-core-5.1 php5-mysql libapache2-mod-php5 php5-common
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  wnms-server*
0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 2,322kB disk space will be freed.
Do you want to continue [Y/n]? y
(Reading database ... 24808 files and directories currently installed.)
Removing wnms-server ...
 * Reloading web server config apache2
WNMS collector 1.2, Oct 21 2011 00:00:44, r30970
                                                                                [ OK ]
Purging configuration files for wnms-server ...
Processing triggers for ureadahead ...
tester@ubuntu:~$
```

Step 2. **Uninstall WNMS collector**. Type command

```
sudo apt-get purge wnms-collector
```

```
test@ubuntu:~$ sudo apt-get purge wnms-collector
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apache2-utils libnet-daemon-perl libhtml-template-perl libdbi-perl mysql-client-core-5.1 apache2.2-bin
  libdbd-mysql-perl mysql-server-5.1 libapr1 mysql-client-5.1 mysql-common libaprutil1-ldap
  apache2-mpm-prefork libplrpc-perl mysql-server-core-5.1 libaprutil1-dbd-mysql apache2.2-common ssl-cert
  libmysqlclient16 php5-mysql libapache2-mod-php5 libaprutil1 php5-common
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  wnms-collector*
0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 176kB disk space will be freed.
Do you want to continue [Y/n]? y
```

Choose option **Y**(yes), to remove collector:

```
test@ubuntu:~$ sudo apt-get purge wnms-collector
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apache2-utils libnet-daemon-perl libhtml-template-perl libdbi-perl mysql-client-core-5.1 apache2.2-bin
  libdbd-mysql-perl mysql-server-5.1 libapr1 mysql-client-5.1 mysql-common libaprutil1-ldap
  apache2-mpm-prefork libplrpc-perl mysql-server-core-5.1 libaprutil1-dbd-mysql apache2.2-common ssl-cert
  libmysqlclient16 php5-mysql libapache2-mod-php5 libaprutil1 php5-common
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  wnms-collector*
0 upgraded, 0 newly installed, 1 to remove and 3 not upgraded.
After this operation, 176kB disk space will be freed.
Do you want to continue [Y/n]? y
(Reading database ... 24664 files and directories currently installed.)
Removing wnms-collector ...
 * Reloading web server config apache2                                                    [ OK ]
Purging configuration files for wnms-collector ...
Processing triggers for ureadahead ...
tester@ubuntu:~$
```

Step 3. The WNMS system has been successfully uninstalled.

WNMS Virtual Image

WNMS is also available as a VMware virtual image which can be run on Windows and others operating systems. Virtual machine option is a quick way to start and familiarize with WNMS, and try all its advantages. Moreover, such virtual method can be used for normal WNMS operation. WNMS virtual image can be easily played with VMware player or VirtualBox.

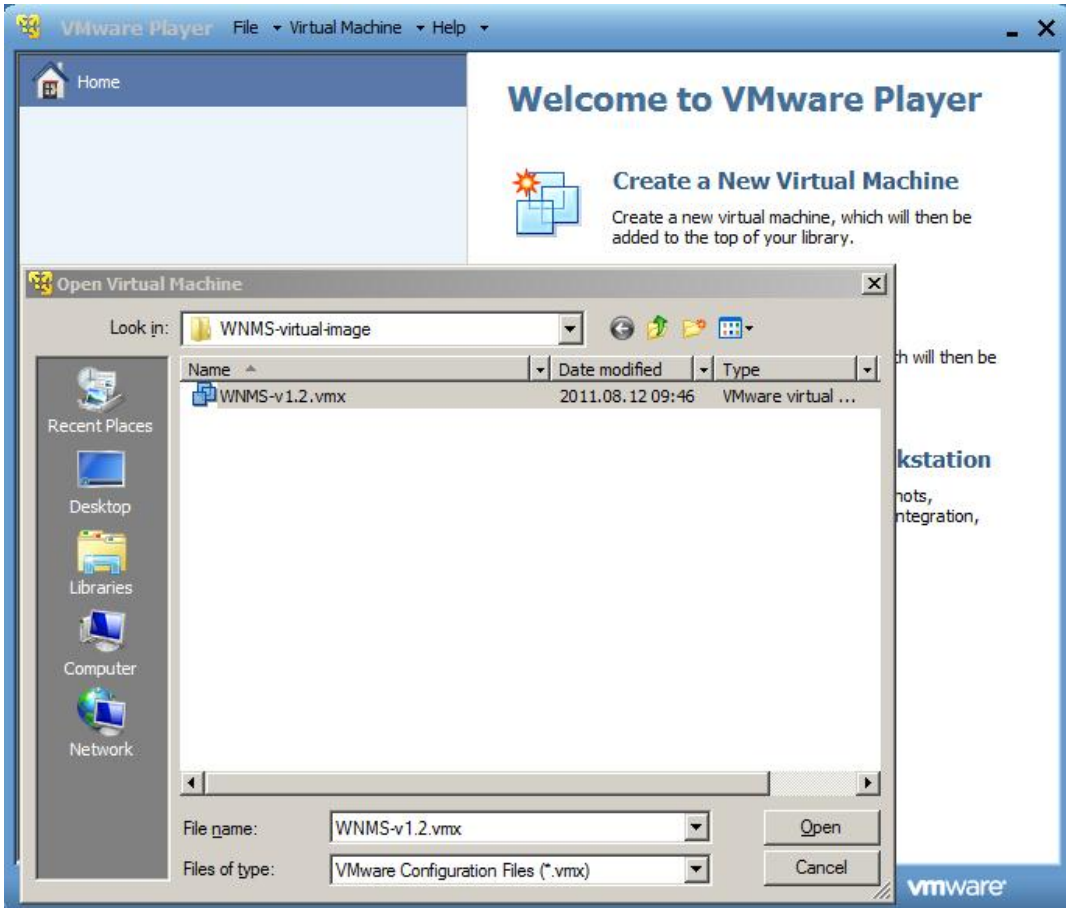
WNMS setup with VMware player

This example covers how to setup WNMS as virtual system on Windows.

Step 1. Download and install VMware player.

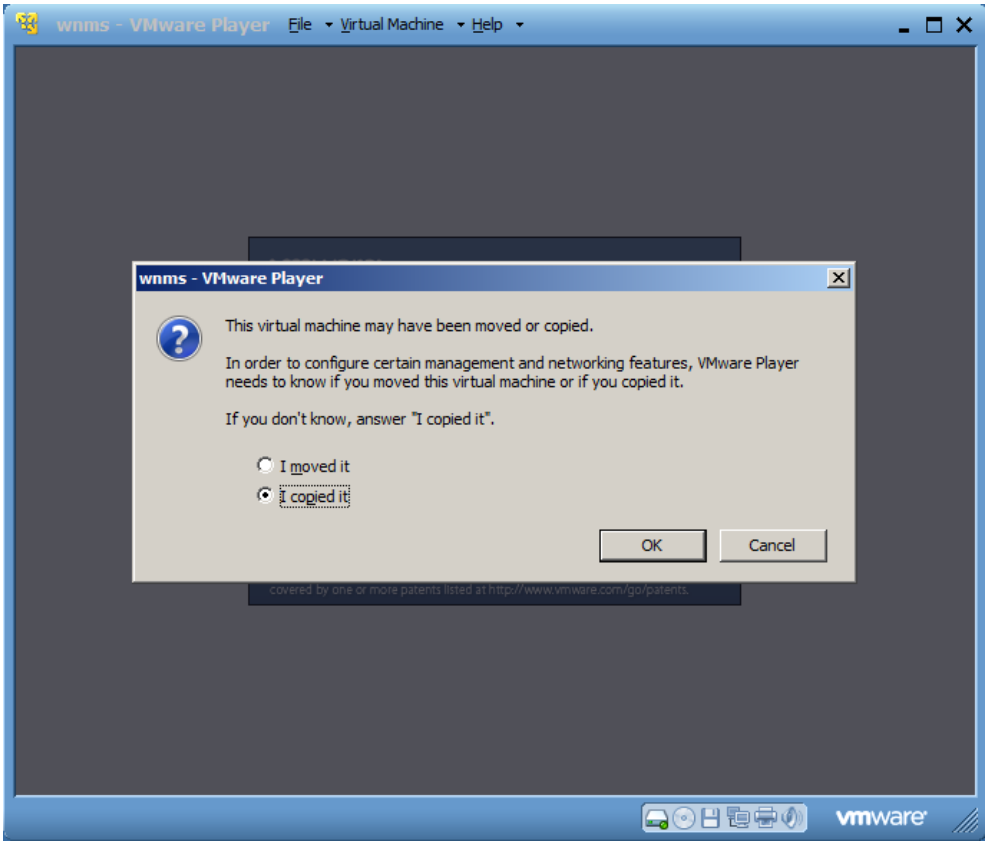
Step 2. Download WNMS virtual image from LigoWave page www.ligowave.com and extract it.

Step 3. Start VMware player, choose **Open a Virtual Machine**, locate WNMS virtual image folder, select configuration file **wnms.vmx** and press **Open**.

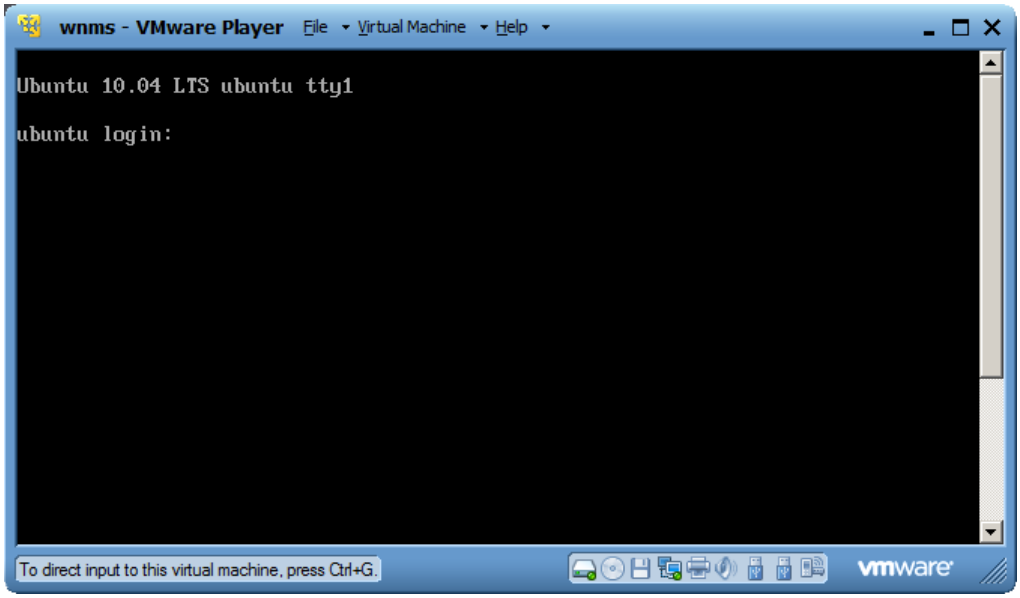


Step 4. Select WNMS on home window and press **Play virtual machine**.

Step 5. If the system asks about system status, leave it as copied. VMware may suggest installing of additional tools – this is optional.



Step 6. You should see a following window if the system started successfully.



WNMS server is based on Linux. Login settings to the server console are:

- Username: **wnms**
- Password: **admin01**

WNMS server is preconfigured with static IP address `192.168.2.66/255.255.255.0`. VMware machine virtual network adapter is set to bridged mode.

Step 7. Change WNMS IP settings according to your subnet: login to the server console, load Interfaces file by command

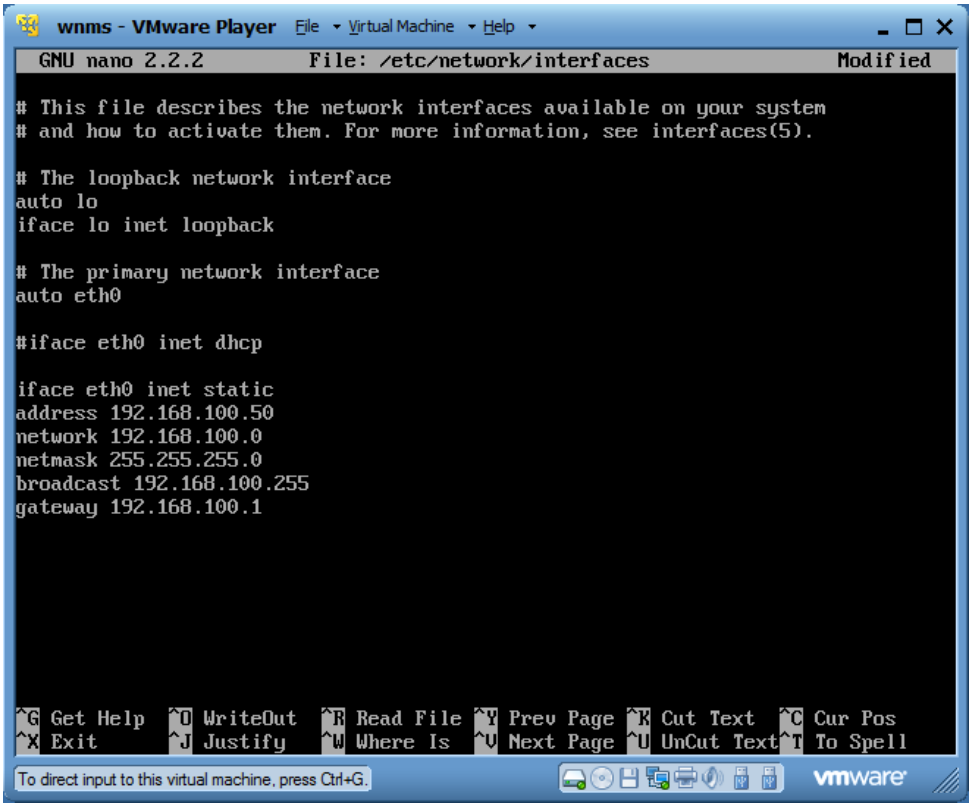
`sudo nano /etc/network/interfaces ,`

then specify the default password **admin01** and change the default IP address to custom, according your subnet.

Depending on host operating system, you may use `Ctrl+ N/P/F/B` keys combinations instead of arrows for moving a cursor

Step 8. After changes on IP settings, reboot WNMS, execute command:

`sudo reboot`



Step 9. Access WNMS GUI by configured IP address (in our example this would be `http://192.168.100.50/wnms`).

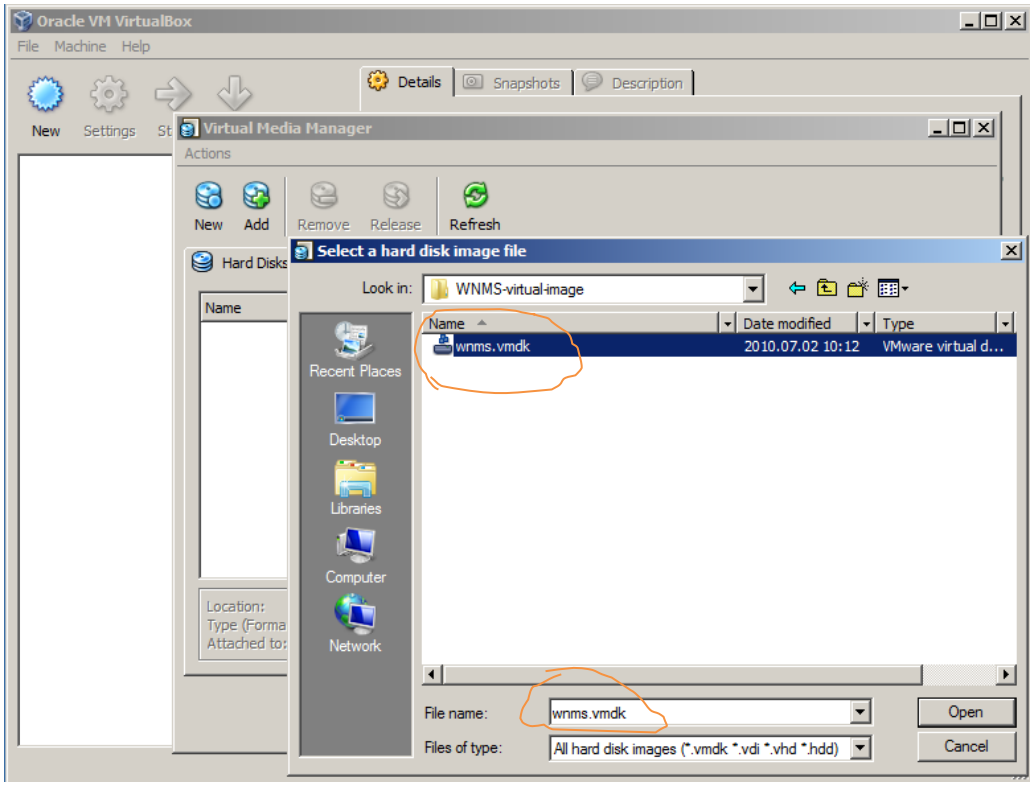
WNMS Setup with VirtualBox

This example covers how to setup WNMS as virtual system on Windows.

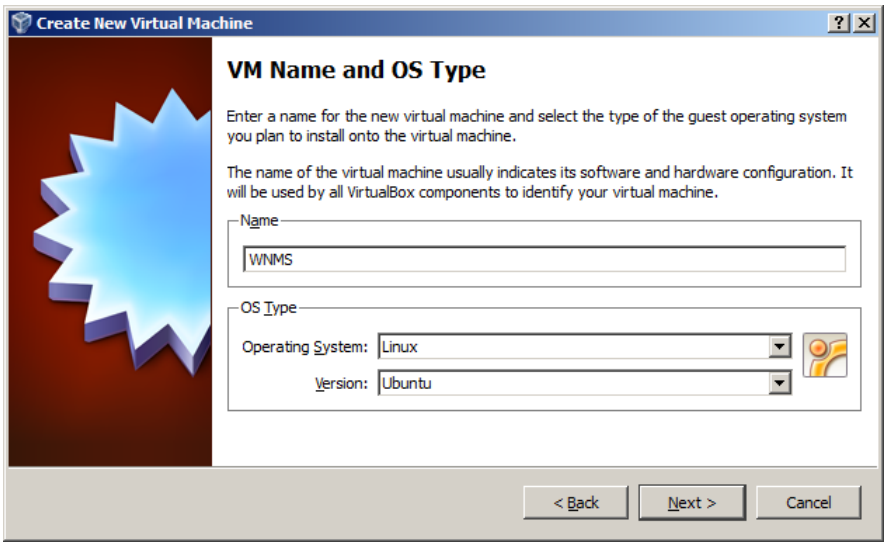
Step 1. Download and install VirtualBox machine.

Step 2. Download WNMS virtual image from LigoWave page www.ligowave.com and extract it.

Step 3. Start VirtualBox machine, go to **File->Virtual Media Manager**, choose **Add**, locate WNMS virtual image folder, select **wnms.vmdk** and press **Open**, then **OK**.



Step 4. Choose **New** to start Virtual Machine Wizard, press **Next**. Write name of virtual machine and select operating system **Linux Ubuntu**. Press **Next**, choose **512 MB** of memory.

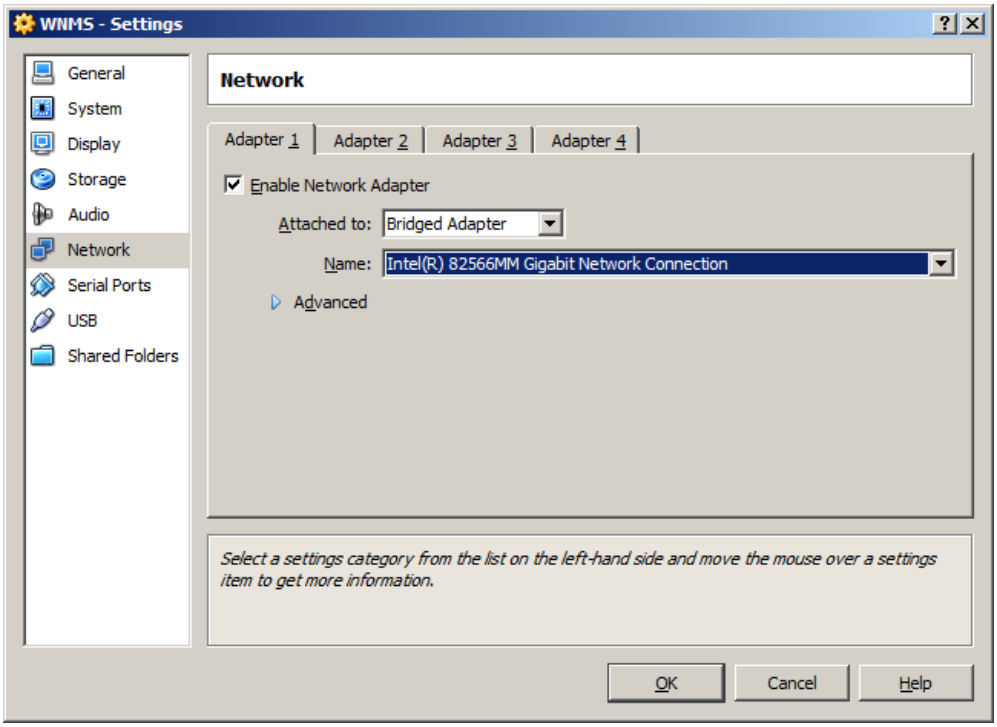


On virtual hard disk section select **Use existing hard disk wnms.vmdk**

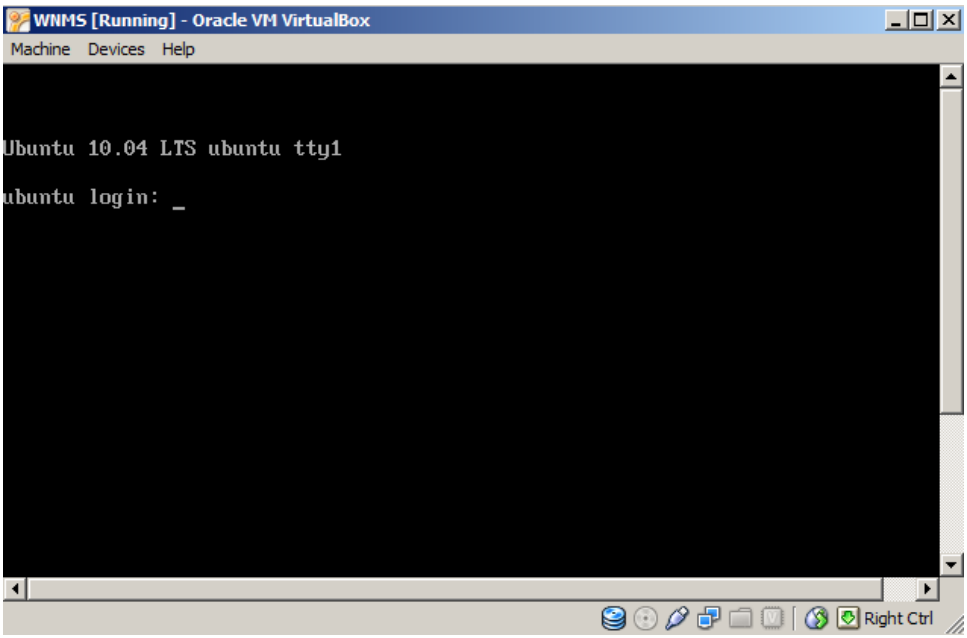
(normal, 20 GB)

Press **Next** and **Finish**.

Step 5. Go to **Settings** of newly created virtual machine, choose **Network**, change NAT to **bridged adapter** and select proper physical network card. Press **OK**.



Step 6. Press **Start** to boot your WNMS server. You shall get following screen on success:



For IP address configuration on WNMS server refer to the previous section *WNMS setup with VMware player*, **Step 7**.

Upgrade from previous version

1. Login to your virtual machine console. Default username is “wnms” and default password is “admin01”
2. Refer to the linux upgrade section. An upgrade procedure is the same

Device Management

Access the WNMS Server

The WNMS server installation generates a system administrator's account so you can access your WNMS server with default login settings on the first connection to the WNMS server.

Default login settings are:

- Username: **admin**
- Password: **admin01**

Open a Web browser, type the server's IP address where the WNMS is installed (e.q. `http://192.168.2.131`) and the login page will be displayed:

Figure 2 – WNMS Server Login Page

Enter the user's login details as requested and log on the WNMS server.

Log Out

To leave the WNMS server, click the **Log Out** link at the top right corner of the page and you will be redirected to the WNMS server login page.

Device Registration

Check if your system meets conditions for proper communication between devices and WNMS server:

1. Properly installed WNMS server (refer to the WNMS Installation Guide)
2. The WNMS Agent must be enabled on each through device web management interface:

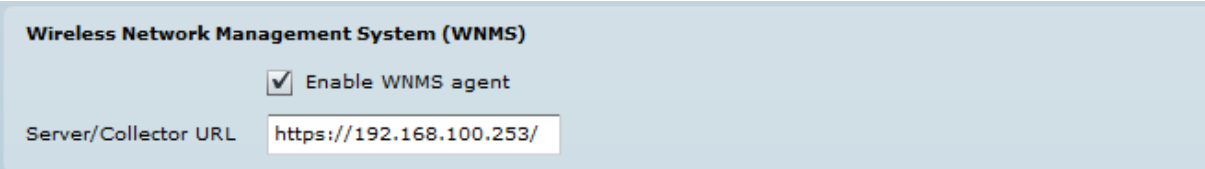


Figure 3 – WNMS Agent Configuration on Device GUI

It is recommended to use `https` protocol for secure communication between agent and server.

By default newly connected devices get “Unregistered” state on WNMS server. Follow the steps to register device manually:

Step1. Navigate to the **Inventory | Devices** menu to view list of connected devices to the WNMS server.

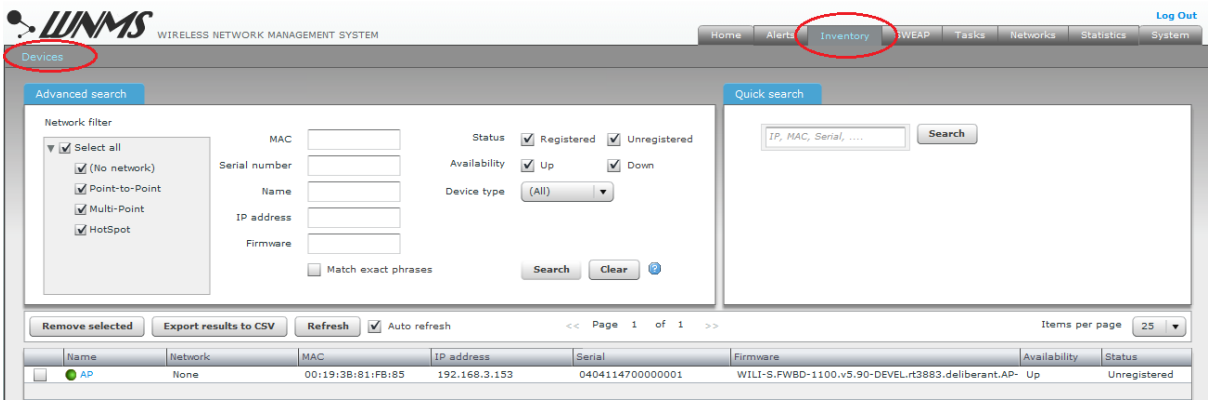


Figure 4 – Device List: unregistered devices

The color of the icon next to the device name indicates alert state (refer to the respective section *Alerts* for information how to setup Alert monitoring on the devices):

- Green icon means that device has no alert or has informational level alerts (active/inactive/closed).
- Yellow icon means that device has active warning level alerts or had in the past critical/warning alerts but now they are closed (not cleared) or had inactive critical/warning alerts (not cleared)
- Red icon means that device has active critical level alerts (not including inactive alerts)

Step 2. A certain **Network** must be assigned for each registered device on the WNMS server. Click on the device name to load the **Device Details** window, choose the network (choose one of the default WNMS networks) for device:

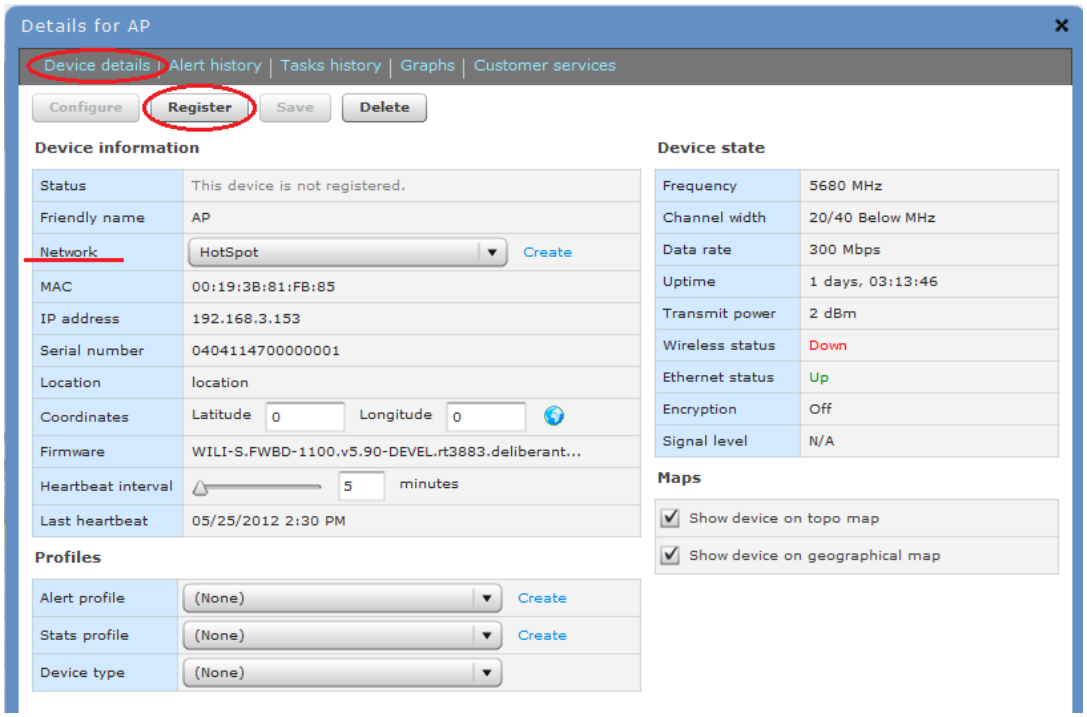


Figure 5 – Device Details: device registration

There are 3 functional buttons that controls device settings:

- **Configure** – click to load regular device web management interface on new web browser's window (direct access to the device is required. Won't work under NAT).
- **Register** – click to register the device. This button is active only if device state is "Unregistered".
- **Save** – saves changes that were made on this page.
- **Delete** – deletes particular device from the WNMS server. If deleted device continues to send heartbeats to WNMS server, it will appear on WNMS server under "Unregistered" state as soon as the first heartbeat will be get.

Step 3. Navigate to the **Customer services** menu and specify the warranty start date:

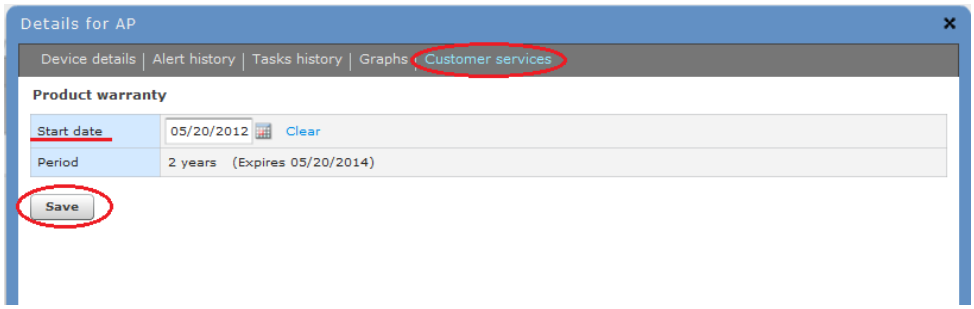


Figure 6 – Device Details: product warranty

Step 4. The registration of the device has been finished successfully:

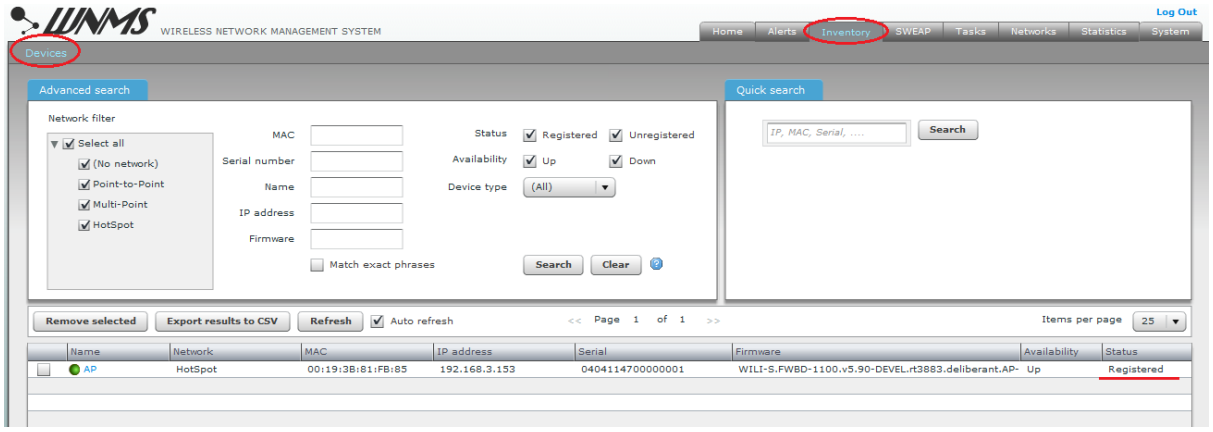


Figure 7 – Device List: successfully registered device

Delete Device

Navigate to device table on the **Inventory | Devices** page, select required devices and click the **Remove Selected** button to delete device:

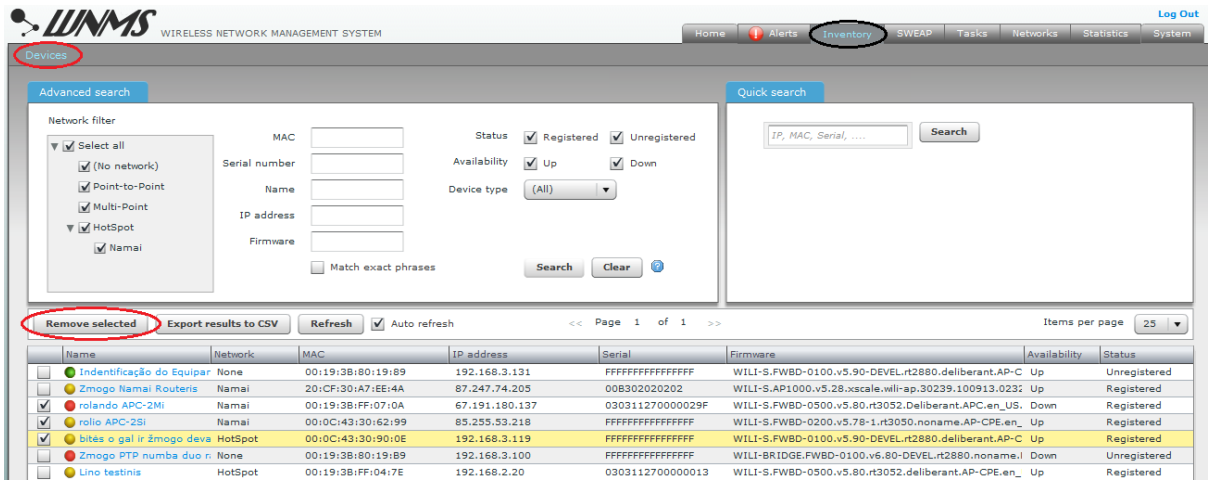


Figure 8 – Delete Device form the WNMS

Deleted device appears on WNMS server with “Unregistered” state if it continues to send heartbeats to the server.

Device Monitoring

There are two main device monitoring tools on the WNMS server:

- **Alerts** – monitor the state and report all alarms received from the device.
- **Statistics in graphs** – gathers and displays graphically chosen statistics.

Alerts

The main WNMS server feature is to gather and display alerts that were sent from devices to the WNMS server using heartbeats.

The source of alerts is the **Alert Profile**, assigned to the device. Alert profiles consist of alerts that are described in Alert Definitions. There are three severity levels of alarms: critical, warning and informational. These alarm's levels are user definable/customizable. WNMS server has two default predefined Alert Profiles, which includes following standard Alert Definitions:

Basic alert profile:

- **Device availability (up/down)** – critical – alerts on device state change: up/down.
- **Ethernet port status** – critical – alerts on Ethernet port state change: up/down.
- **Radio status** – critical – alerts on Radio port state change: up/down.
- **Reboot** – warning – alerts on device reboot.
- **RSSI** – warning – alerts if RSSI threshold is below 20.

Extended alert profile:

- **Device availability (up/down)** – critical – alerts on device state change: up/down.
- **Ethernet port status** – critical – alerts on Ethernet port state change: up/down.
- **Radio status** – critical – alerts on Radio port state change: up/down
- **Reboot** – warning – alerts on device reboot.
- **RSSI** – warning – alerts if RSSI threshold is below 20.
- **Frequency change** – warning – alerts on frequency change.
- **Noise level** – warning – alerts if Noise level is above -80 dBm.
- **RX packet drop %** – warning – alerts if RX packet drop becomes larger than 5%.
- **TX Retry** % – warning – alerts if TX packet retry becomes larger than 5%.
- **Warranty expired** – warning – alerts when the warranty is expired already.
- **Warranty expiring soon** – informational – alerts if warranty expires within a 30 days.
- **Radio peer count** – informational – alerts if number of radio peers is larger than 20.

The threshold of Alert Definition can be changed or a new custom Alert Definition can be created on the **Alerts | Alerts Definitions** page.

The severity of alerts (critical, warning or informational) can be changed on the **Alerts | Alerts Profiles** page, when adding an alert definition to the profile.

Use **Alerts | Alert Profiles** menu to view the full list of alert profiles:

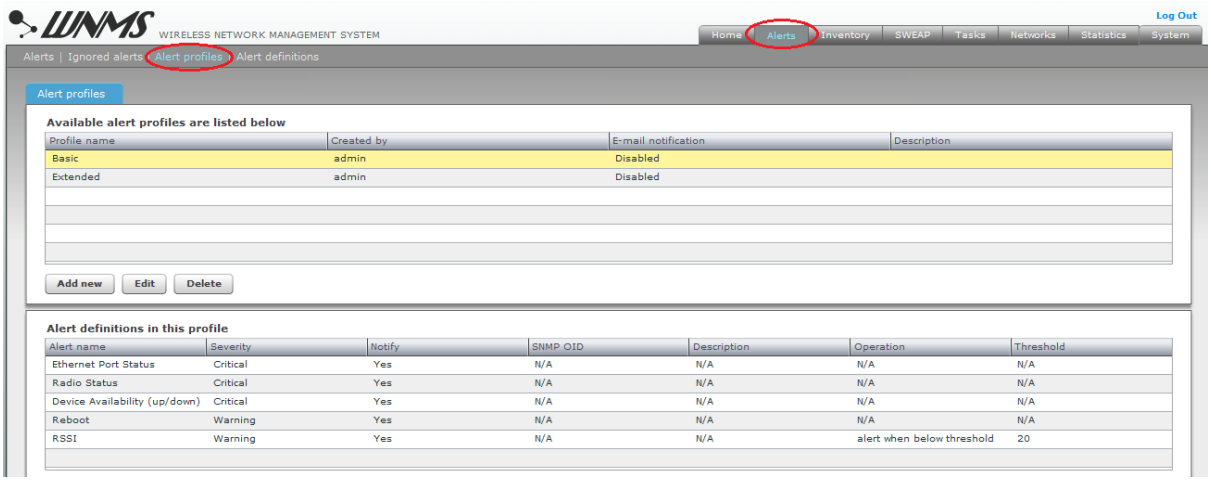


Figure 9 – Default Alert Profiles Table

Follow the steps to enable alert monitoring on the chosen device:

Step 1. Assign the **Alert profile** for the particular the device. Navigate to the **Inventory | Devices** menu, click on your device name and load the device Details window to assign default Alert profile:

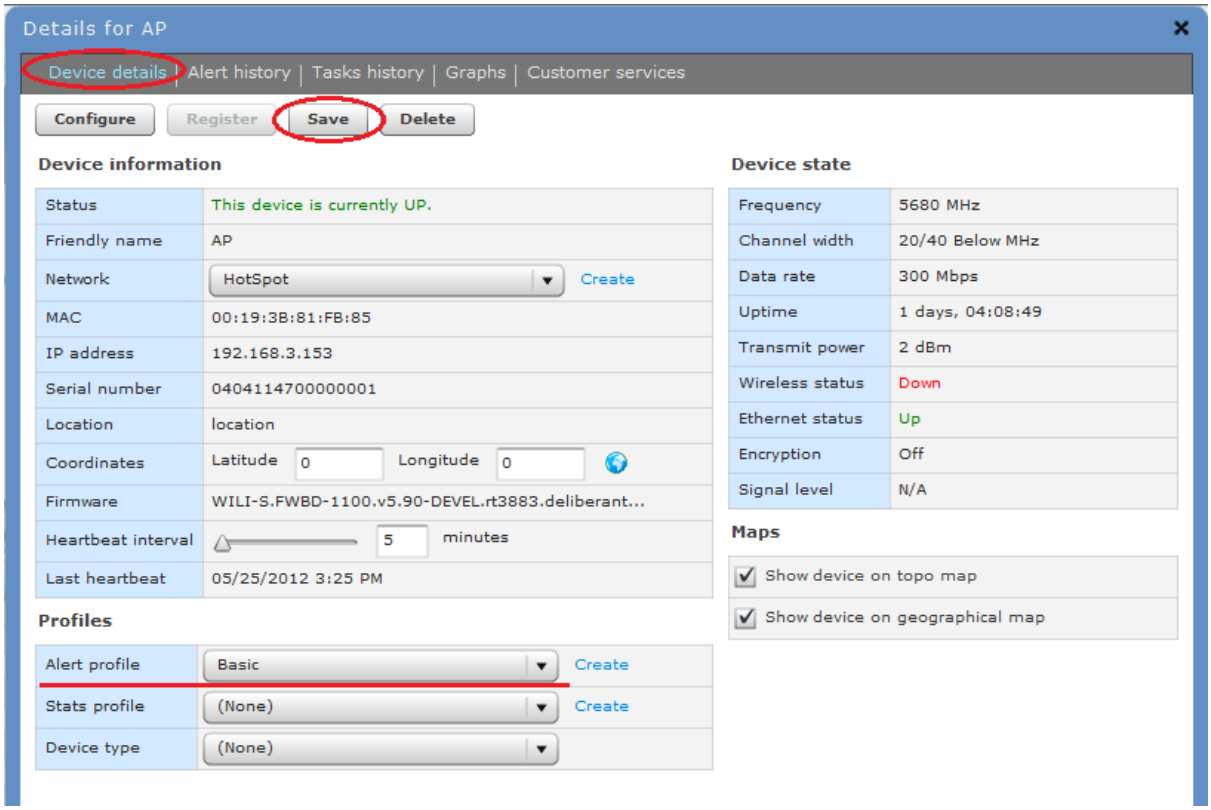


Figure 10 – Assign Chosen Alert Profile.

Step 2. Navigate to the **Alert** menu to view system alerts that were sent by the registered devices. As soon as the correct Alert profile has been assigned to the device, WNMS server starts monitor device alerts that were sent from a device to the WNMS server with each heartbeat.

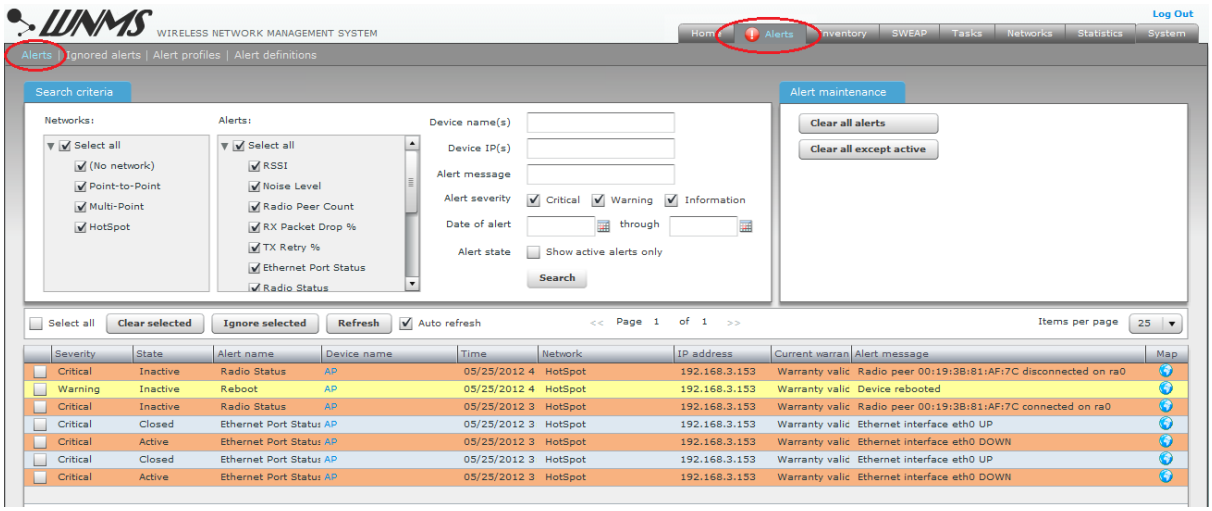


Figure 11 – Alerts Table

The color of alerts indicates alerts severity or closed alerts:
Critical alerts – red color
Warning alerts – yellow color
Informational alerts – green color
Closed alerts – light blue color

A red exclamation sign appears next to Alerts tab when WNMS has active critical or warning alerts (see *Figure 11 – Alerts Table*).

Alerts are grouped into two types having three different **states**:

Active or **Closed** type shows the alerts in two different states: the **Active** state appears when the monitored parameter or value gets back to the normal the **Closed** state appears. For example, if RSSI level of a devices reaches the specified threshold or exceeds it, the alert state becomes active; when RSSI level is lower than the specified threshold, the alert state becomes Closed.

Inactive state shows alerts which have no states, i.e. they cannot get worse or better. Such alerts just inform about the actions which have been performed. There are only three alerts in the Inactive state: Reboot, Frequency Change and Radio status (association/disassociation of Radio Peers).

The outdated alerts can be simply removed from the alerts table by selecting them and using **Clear Selected Alerts** button.

Graphs

The WNMS server is perfect for graphical visualization of device statistical data that was sent from devices to WNMS server with the heartbeats. The main condition, to display graphs of required statistics, is to assign the correct statistics template (default or custom) for the device. Only then WNMS server will start to gather required statistics from the device.

WNMS server has seven predefined default **Statistics Profiles** (Statistics | Statistic Profiles menu) for PTP and APC (AP/CPE) which contains specific **Statistic Definitions**, proper for appropriate product:

- PTP MIMO
- PTP all products
- APC 11n Station
- APC 11n Access Point
- APC 11a/g CPE2/CPE5/AP2i/APsolo
- APC 11a/g AP Duo
- APC 11a/g AP Quad

There is possibility to create custom Statistics Profile, including necessary statistics definitions (build-in or custom) on **Statistics | Statistic profiles** page. The statistics definitions are formed from SNMP OID by adding necessary settings on the **Statistics | Statistic definitions** page. If exact SNMP OID is known, it can by specified directly. Other way is to add SNMP OID from local library.

Follow the steps to setup WNMS server to display a statistics graphically for the device:

Step 1. Assign correct **Statistics profile** for the particular device. Navigate to the **Inventory | Devices** menu, click on your device name and load the device Details window to assign default Statistics profile:

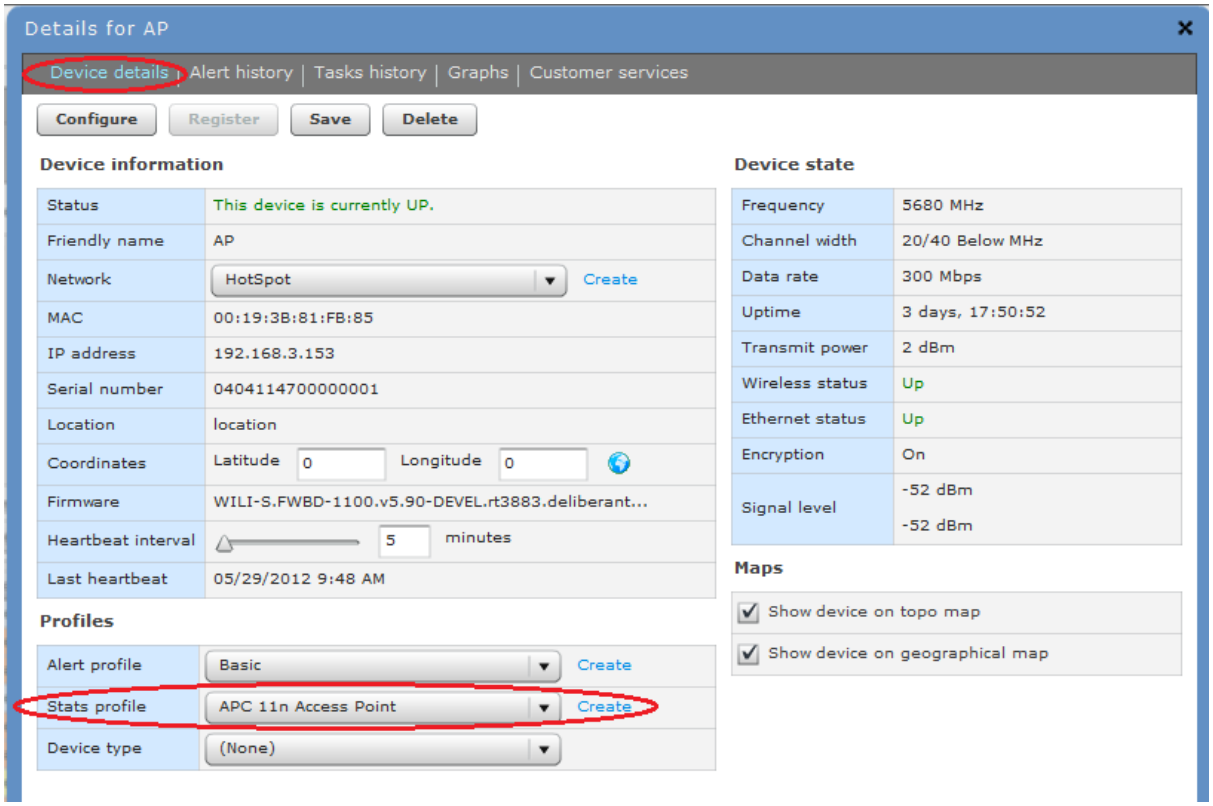


Figure 12 – Device Details: assign statistics profile

It is recommended to use default WNMS Statistics profiles as they are already pre-configured in default WNMS configuration.

Step 2. After the Statistics profile is assigned to the device, need to wait until WNMS server gathers a certain amount of statistical data from the device. Then all the specified graphs can be drawn.

Step 3. Load the **Graphs** menu on the device Details window and the graphs of chosen statistics (specified in the Statistics profile) will be displayed:

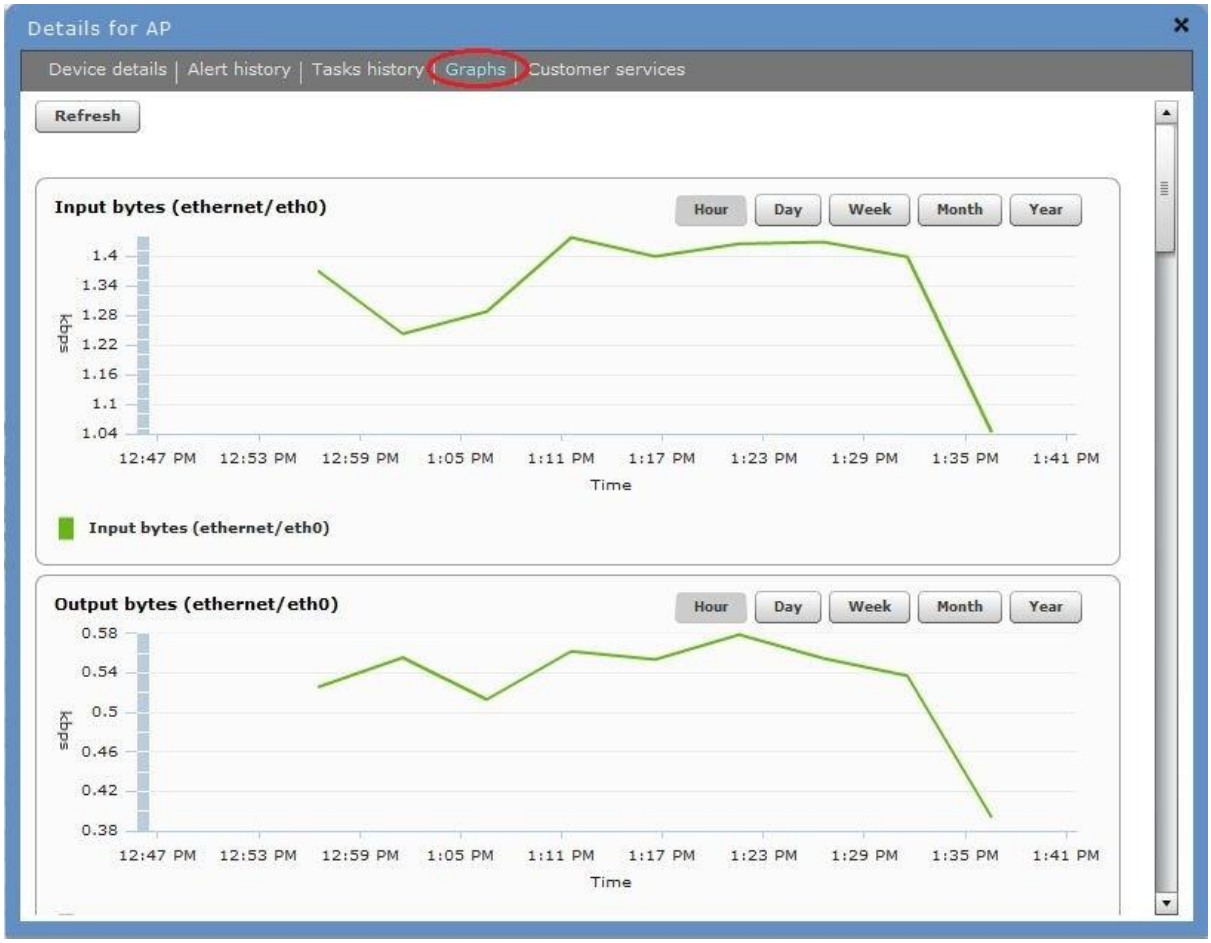


Figure 13 – Device Statistics Graphs

Device Maintainance

The several tasks can be scheduled and performed on devices, registered on the WNMS server:

- Configuration download form the device
- Configuration upload to the device
- Send and **Upgrade firmware** on the device
- Troubleshooting file download from the device
- **Reboot** the device

The new task is created using **Add new** button on the **Tasks** page, which loads a new task creating wizard:

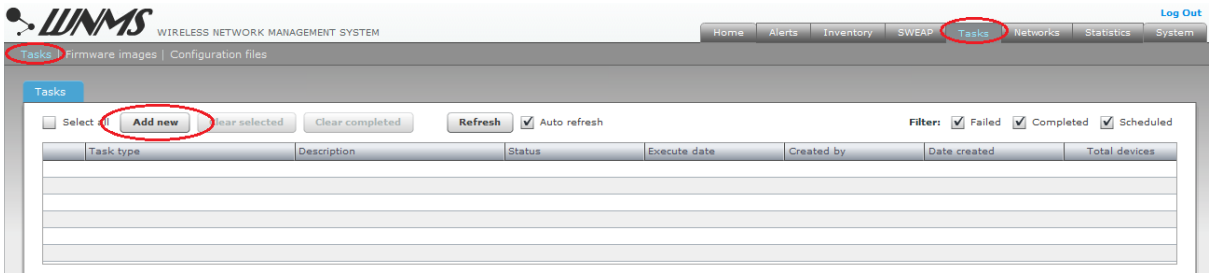


Figure 14 – Tasks Scheduler

Tasks listed in this table have different icons indicating different types of tasks:

- Clock icon means pending tasks. It can indicate either a task which is scheduled to be performed later, or a pending task which has not been performed as the device was offline on the scheduled time (in the latter case the scheduled task will be performed as soon as the device appears online).
- Green icon indicates successfully completed tasks.
- Red icon indicates that task failed.

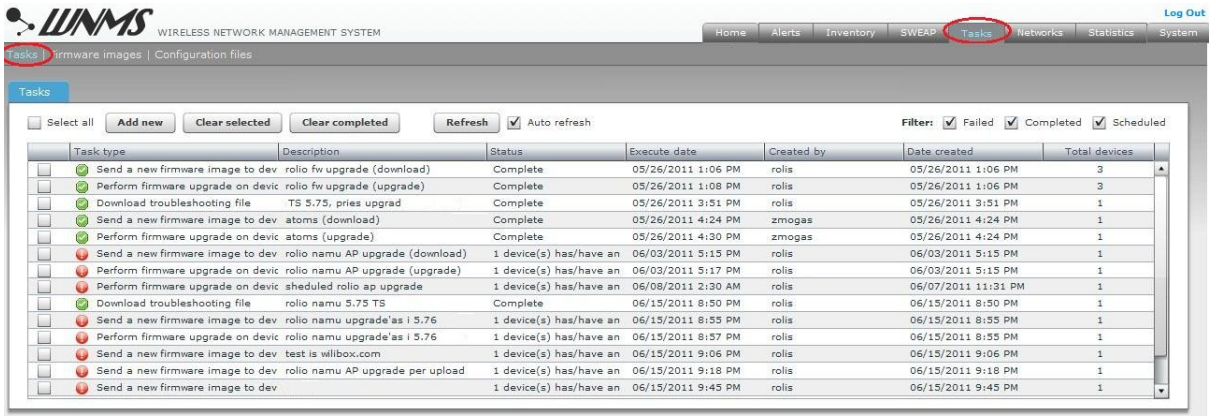


Figure 15 – Table with Different Type of Tasks

Firmware Upgrade

WNMS server has possibility to schedule a remote firmware upgrade for group of devices.

Follow the steps to configure firmware upload and upgrade on the chosen devices:

Step 1. Click the **Add** new button on the **Tasks** page to load the wizard and choose the task type **Send firmware and upgrade**:

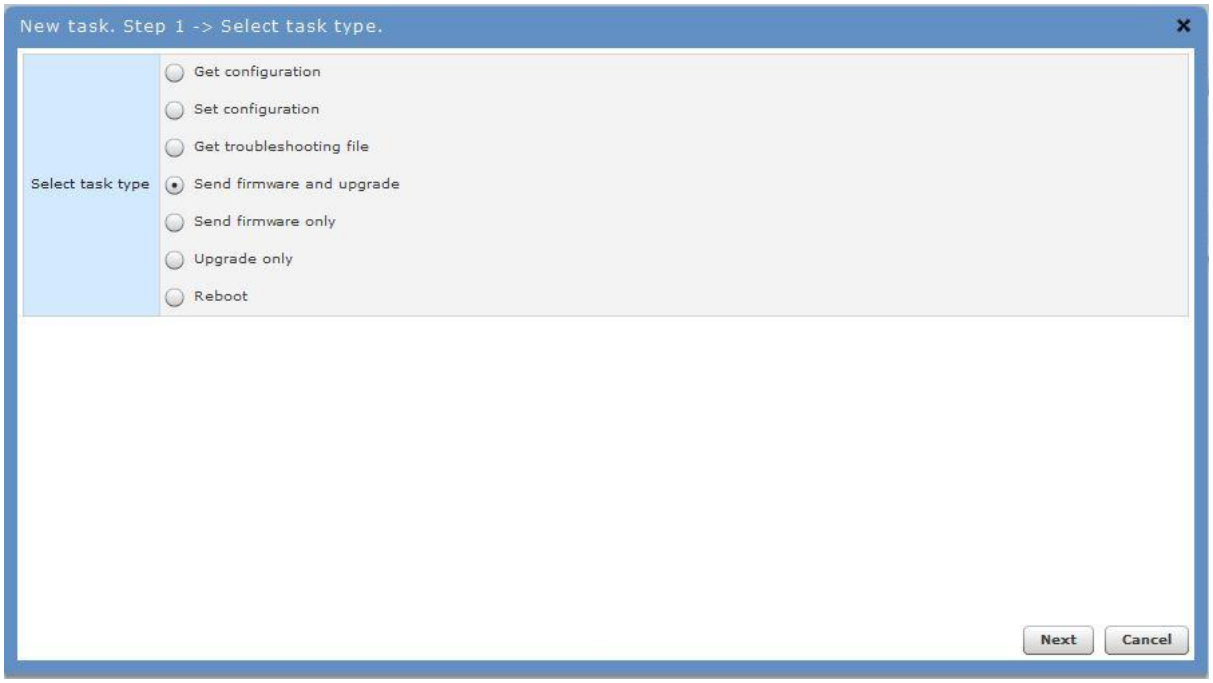


Figure 16 – Schedule Firmware Upgrade on Devices

The WNMS server has possibility to store binary firmware images (under the **Tasks | Firmware images** menu).

Step 2. Specify the details for this task: shedule firmware image upload and upgrade to the device, also specify the firmware image from local PC.

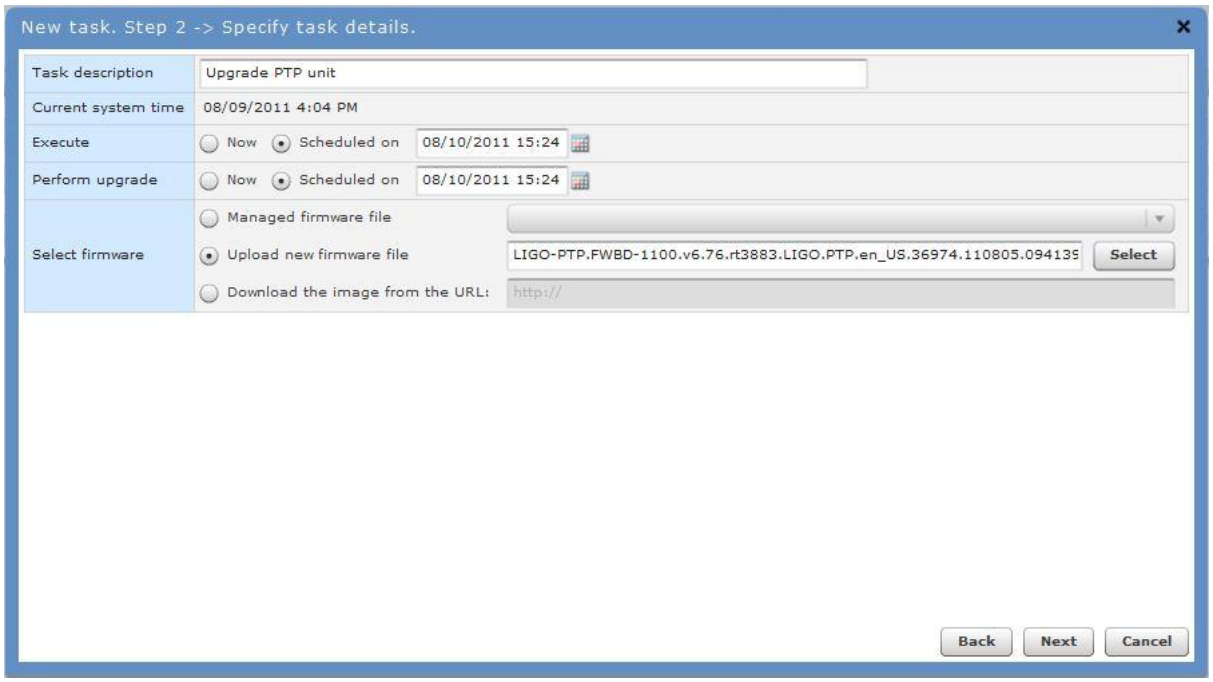


Figure 17 – Enter Task Details

Step 3. Select devices that will be upgraded with the new firmware image: click **Search for devices** button and select required units:

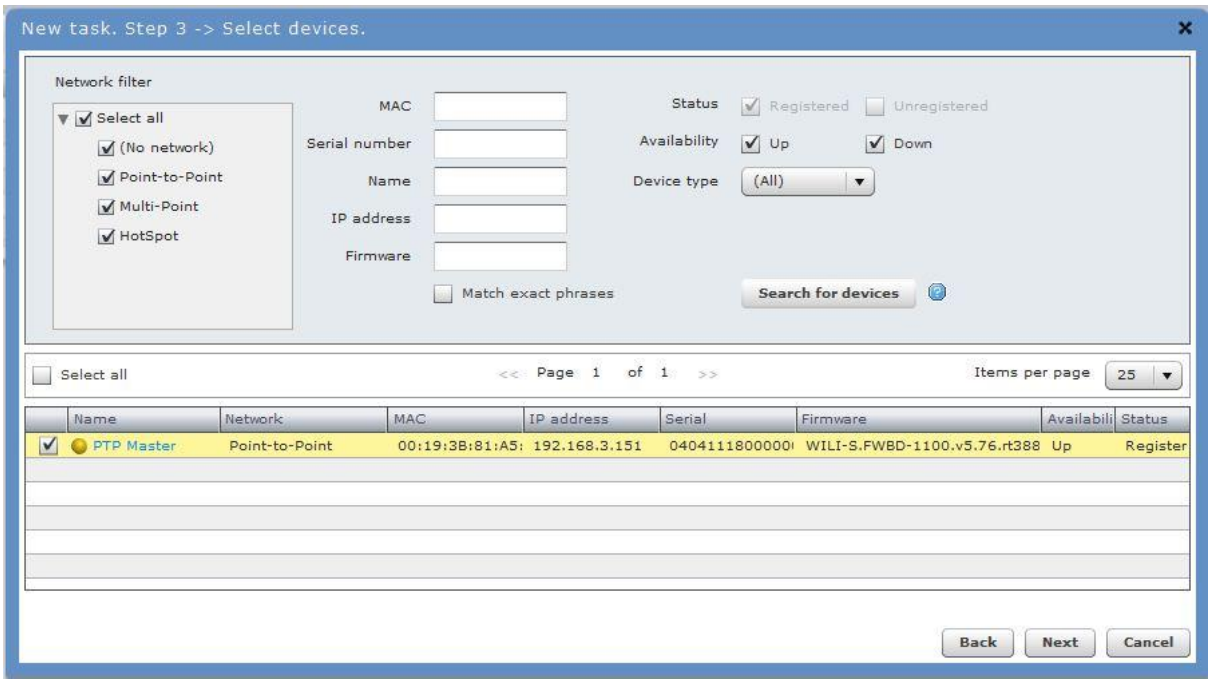


Figure 18 – Select Devices for the Task

Step 4. Confirm newly created firmware upgrade task by clicking the **Finish** button. According this task, the chosen firmware image will be uploaded on selected device on 08-10-2011 03:24 PM.

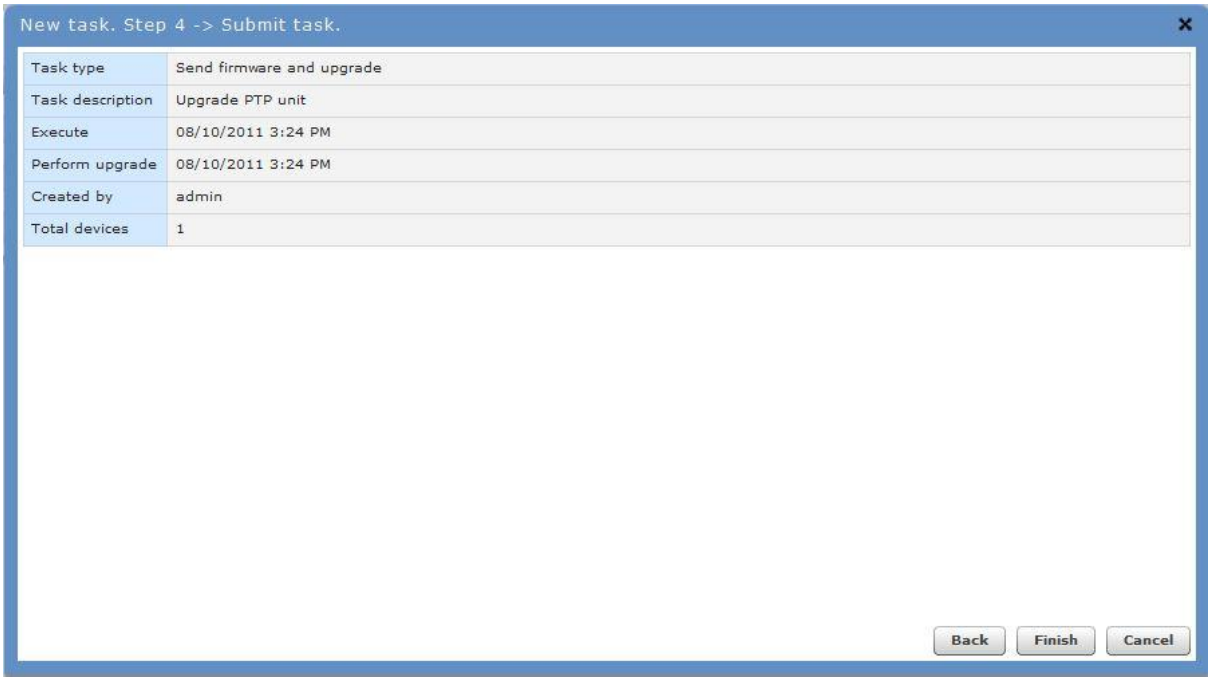


Figure 19 – Task Details

Step 5. Open **Tasks** page and check if new task exists on Task table with clock icon (pending task):

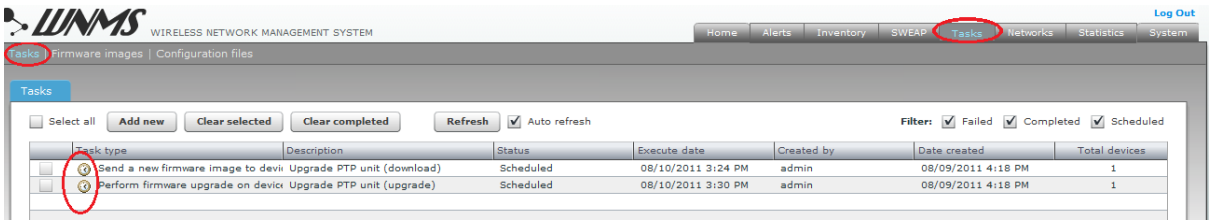


Figure 20 – Task Table: pending scheduled tasks.

Configuration File Download

Follow the steps to download configuration files from chosen devices:

Step 1. Click the **Add** new button on the **Tasks** page to load the wizard and choose the task type **Get configuration** from device:

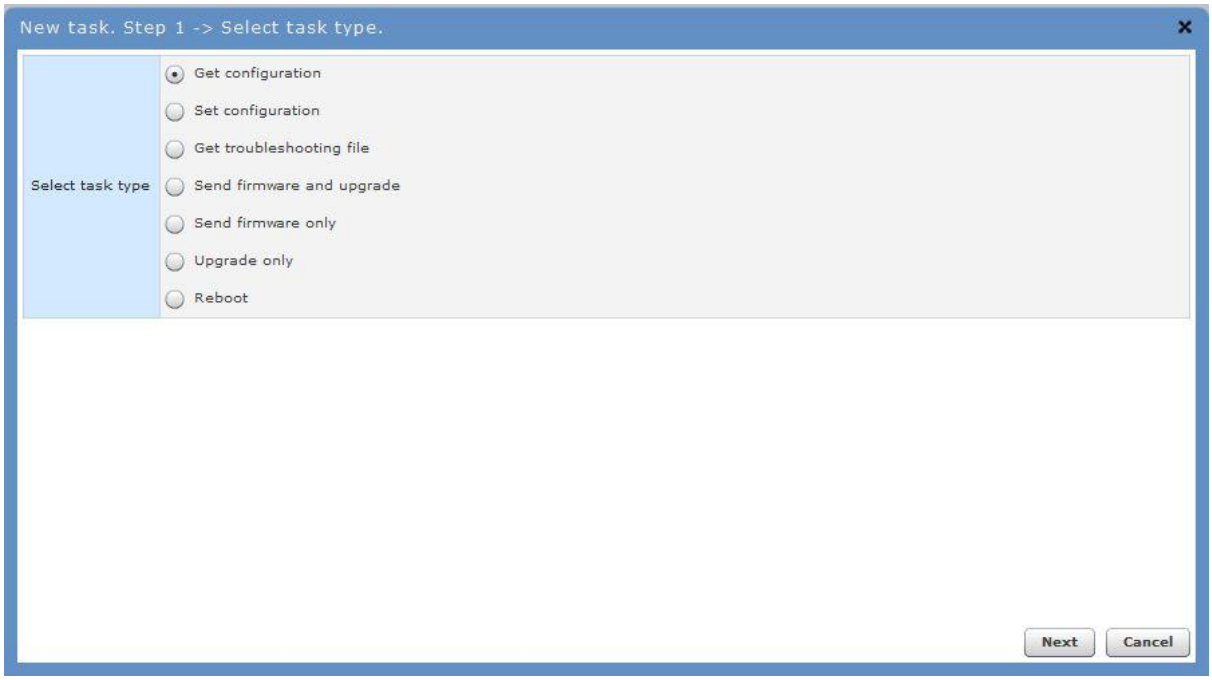


Figure 21 – Schedule Configuration File Download from Devices

Step 2. Shedule task: choose **Now** option to perform this task immediately.

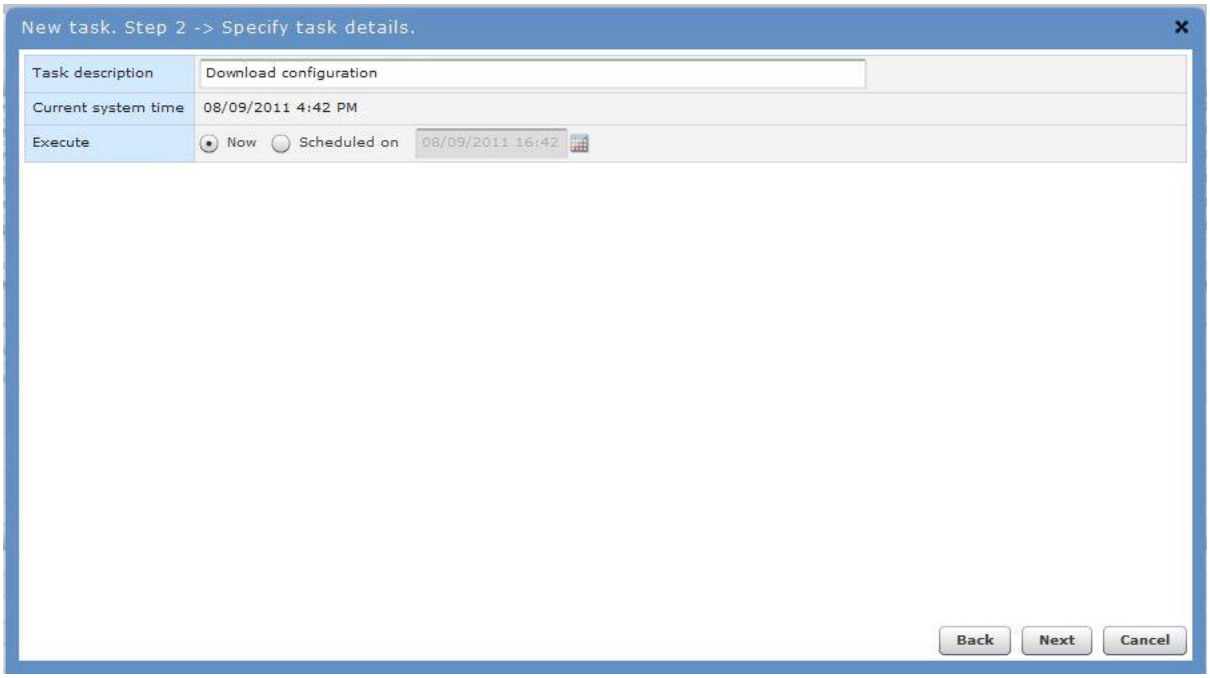


Figure 22 – Enter Task Details

Step 3. Select the devices from which the configuration files will be downloaded to WNMS server: click **Search** button and select required devices.

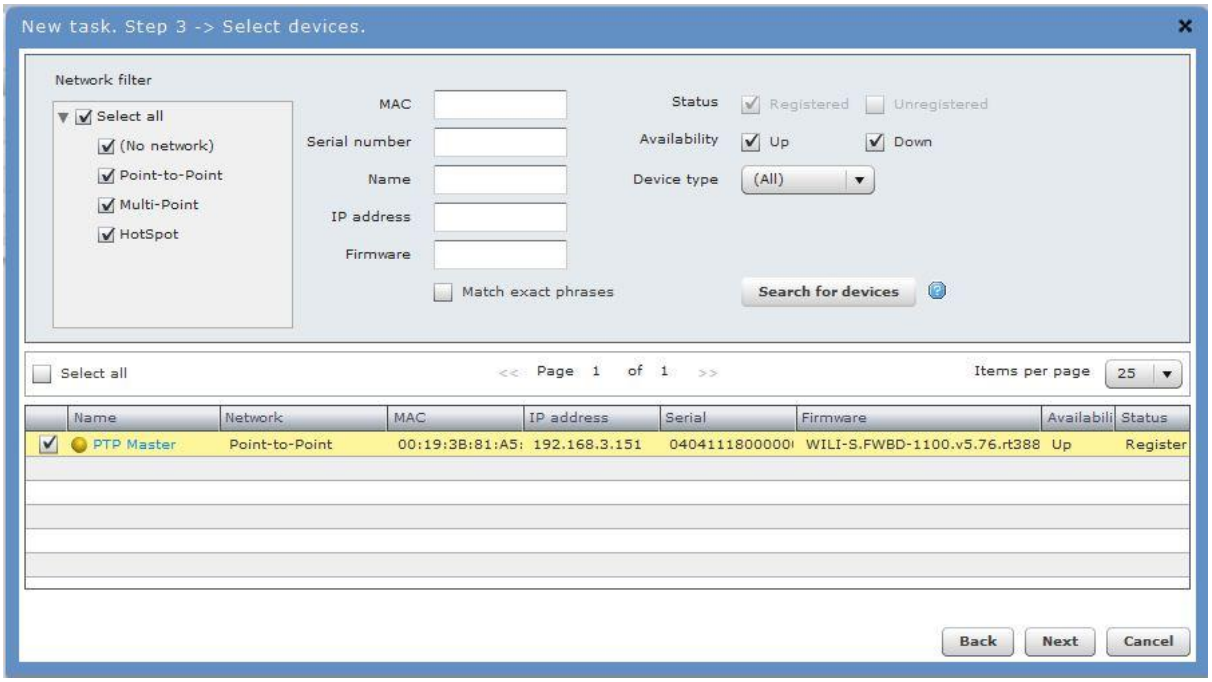


Figure 23 - Select Devices for the Task

Step 4. **Save** newly created task.

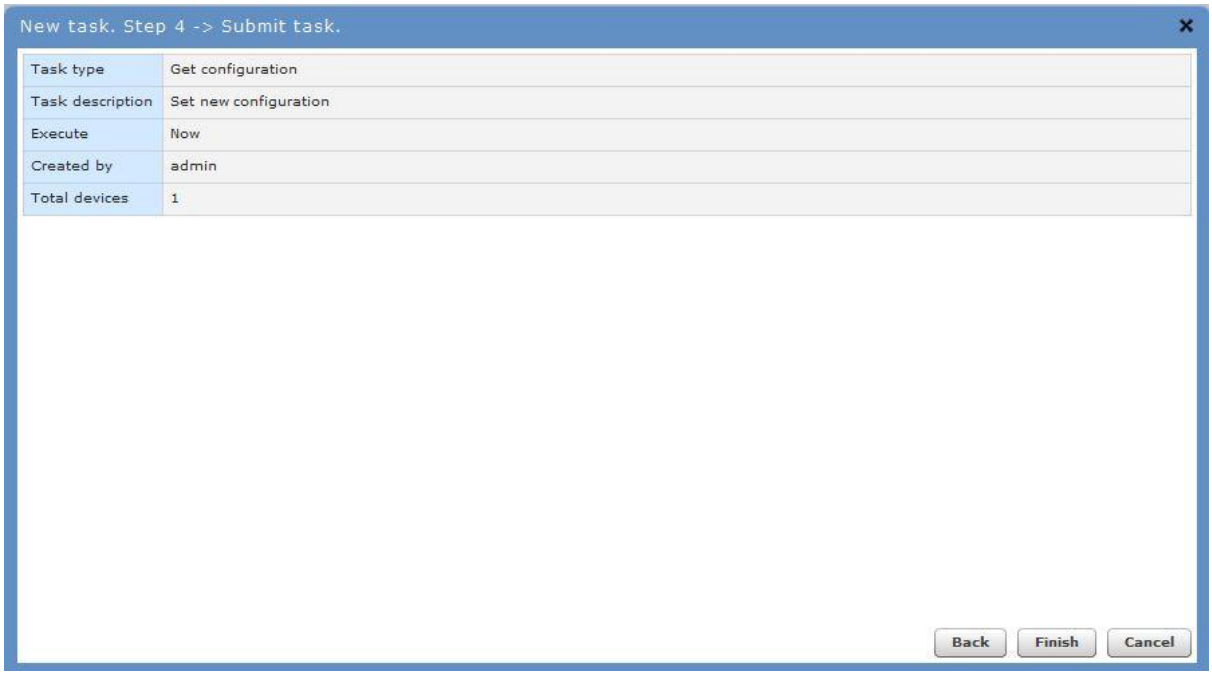


Figure 24 – Task Details

Step 5. Open **Tasks** page and check if new task has been completed successfully (green icon). Select it and the task details will be loaded on the table below. It is now available to view or download the configuration file locally:

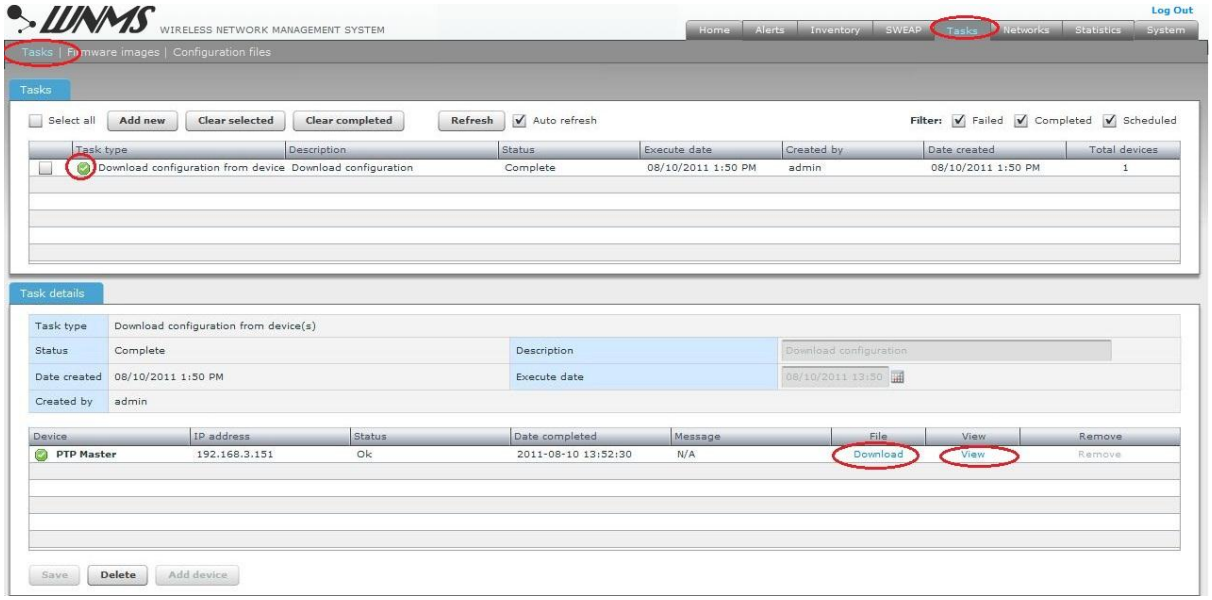


Figure 25 – Task Table: completed download configuration task.

Configuration File Upload

The WNMS server can upload configuration files for chosen devices remotely.

Follow the steps to upload configuration file (stored on administrator‘s PC) on a chosen device:

Step 1. Click the **Add** new button on the **Tasks** page to load the wizard and choose the task type **Set configuration**:

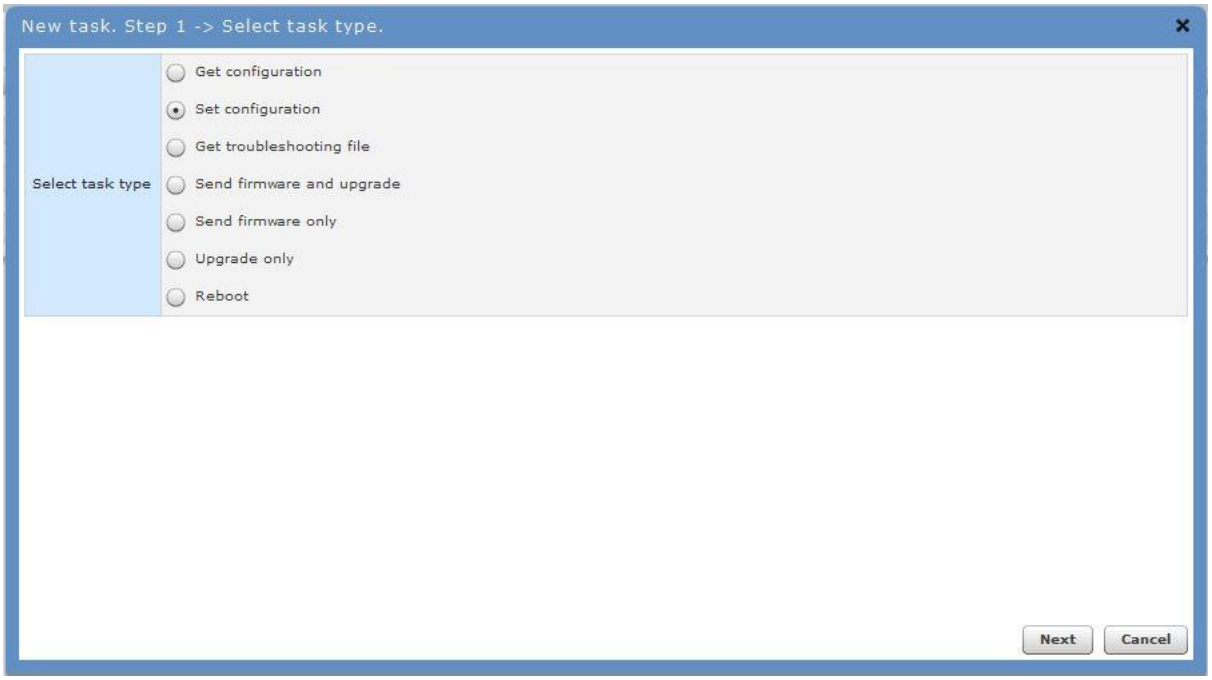


Figure 26 – Schedule Configuration File Upload on Devices

The WNMS server has possibility to store configuration files (under the **Tasks | Configuration Files** menu).

Step 2. Specify the details for this task: schedule configuration file upload to the device, select the file which will be uploaded and choose to reboot the device after configuration upload.

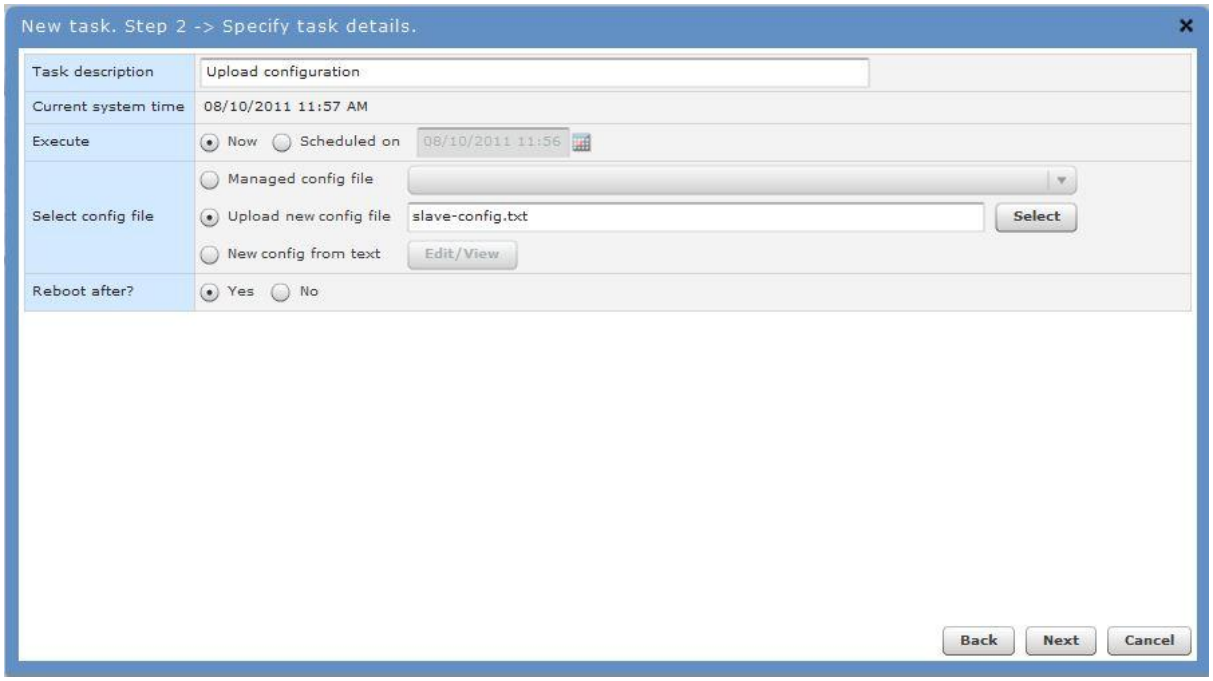


Figure 27 – Specify Task Details

If faulty configuration is uploaded to a device it may cause unexpected behavior or failure of the device.

Step 3. Select devices on which the configuration file will be uploaded: click **Search for devices** button and select required device.

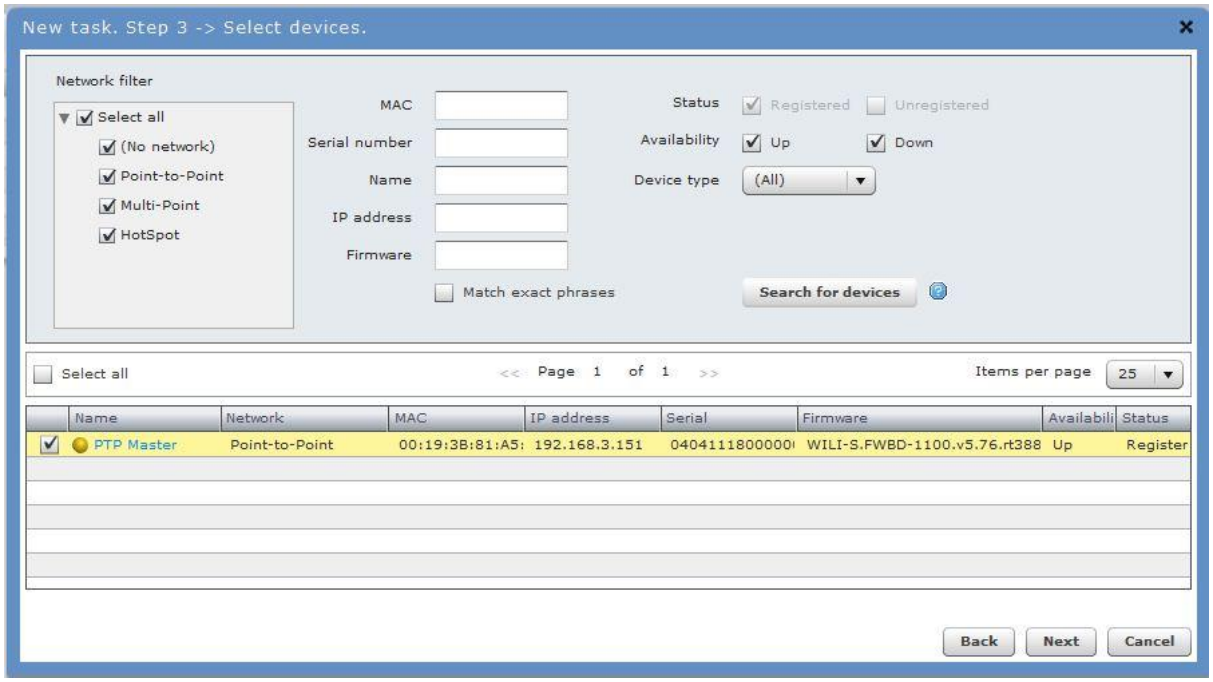


Figure 28 – Select Devices for the Task

Step 4. **Save** newly created task.

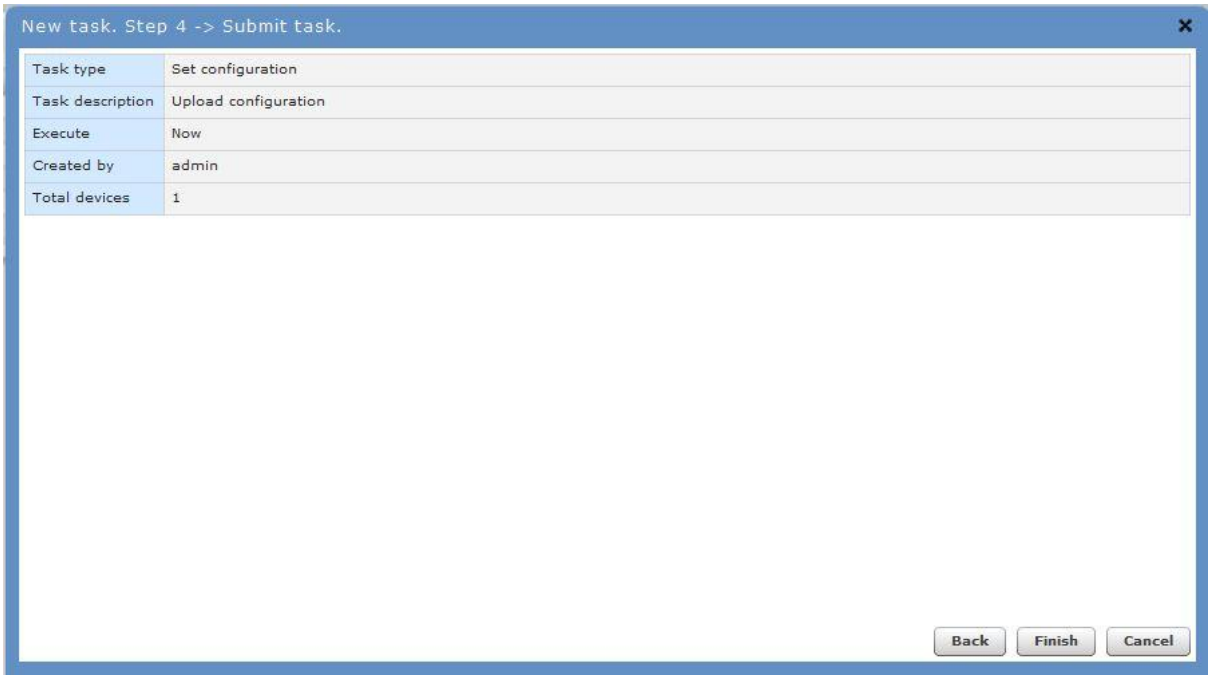
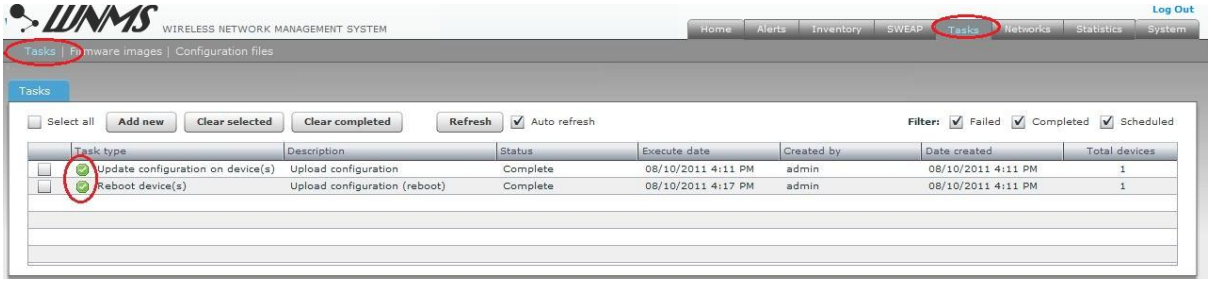


Figure 29 – Task Details

Step 5. Open **Tasks** page and check if new task has been completed:



Network Maps

WNMS has tools for graphical representation of network topology and status of registered devices on WNMS server.

Follow the steps to enable graphical network representation of registered devices on maps:

Step 1. Check if the **Maps** options are enabled on particular device **Details** pop-up window, on **Inventory | Devices** page.

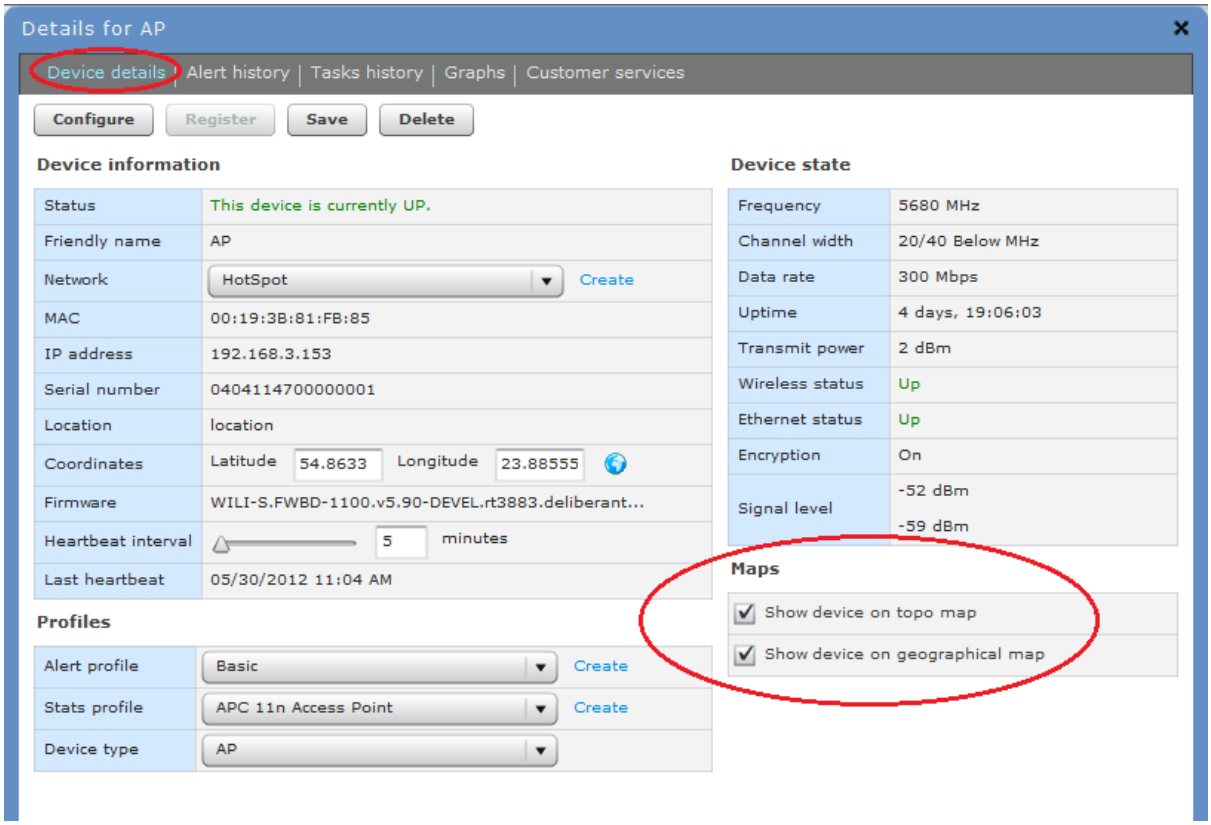


Figure 30 – Device Details: enable maps options

- **Show device on topo map** – enable this option for network topology visualization.
- **Show device on geographical Map** – enable this option for device network visualization on geographical map.

Step 2. It is important to specify the location coordinates (longitude and latitude) on **Device Details** window for graphical representation.

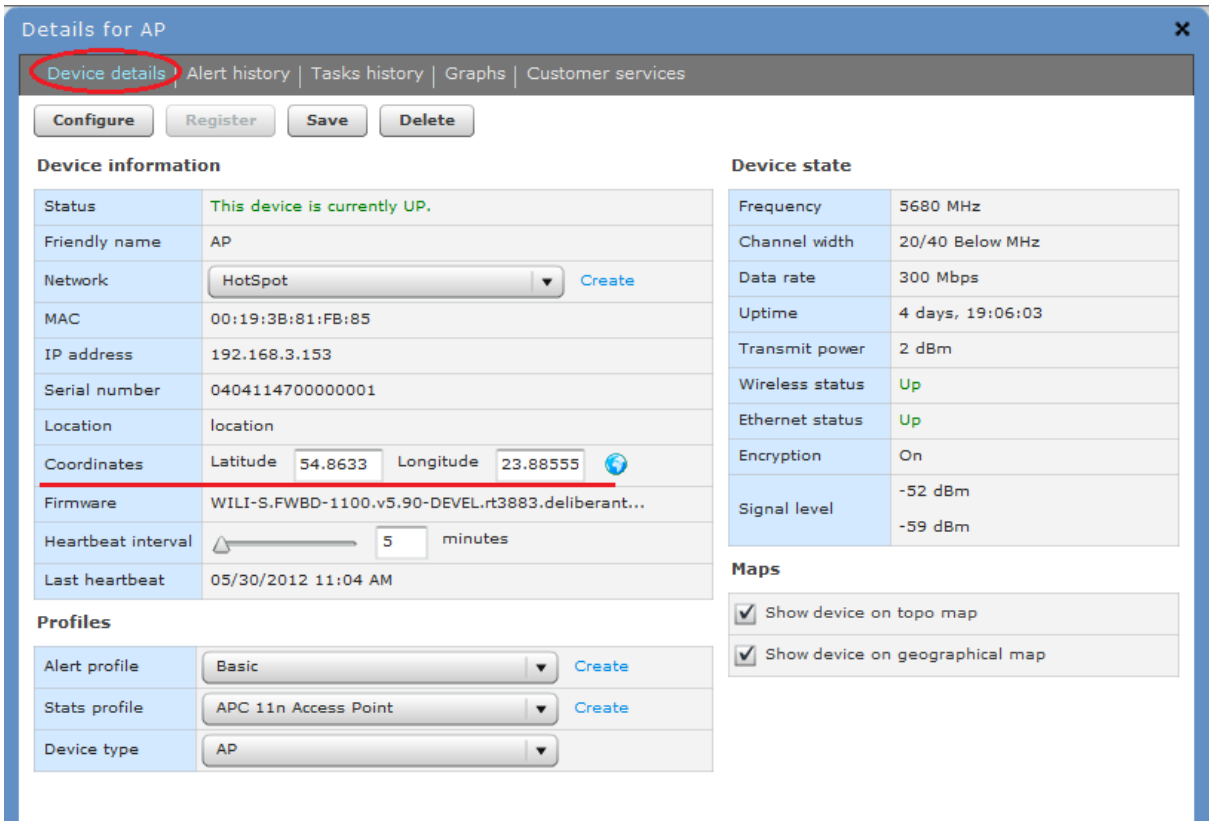


Figure 31 – Device Details: coordinates

WNMS server will get the coordinates with device heartbeat automatically if they are specified in the device configuration and have not been set on WNMS server. Otherwise the coordinates must be specified manually on **Device Details** pop-up window.

Step 3. Specify the **Device type** (AP, CPE, PTP or other) for clear graphical representation on maps, as each type will be displayed in different icons.

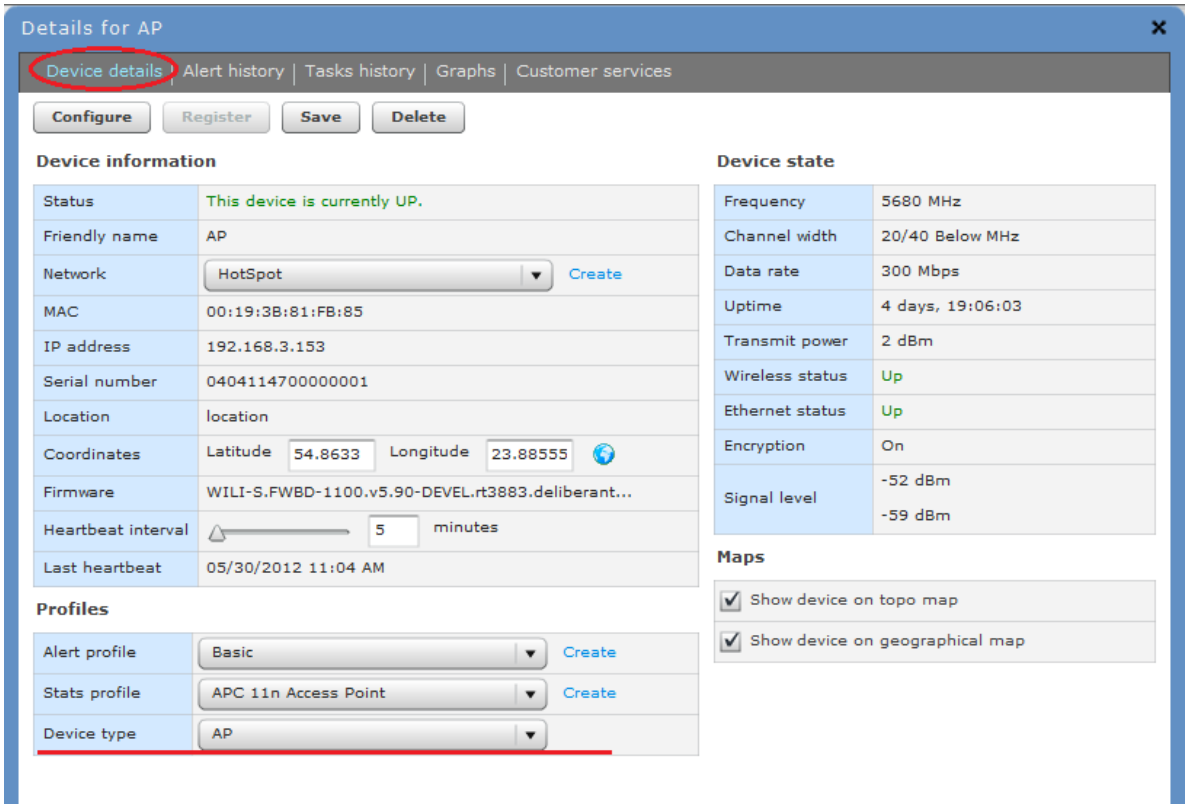


Figure 32 – Device Details: type of the device

Step 4. Navigate to the **Networks | Map** menu; select all options on **Map filter**, select required networks, and click **Apply filters / Refresh** button. The representation of your selected network will be displayed geographically on the map:

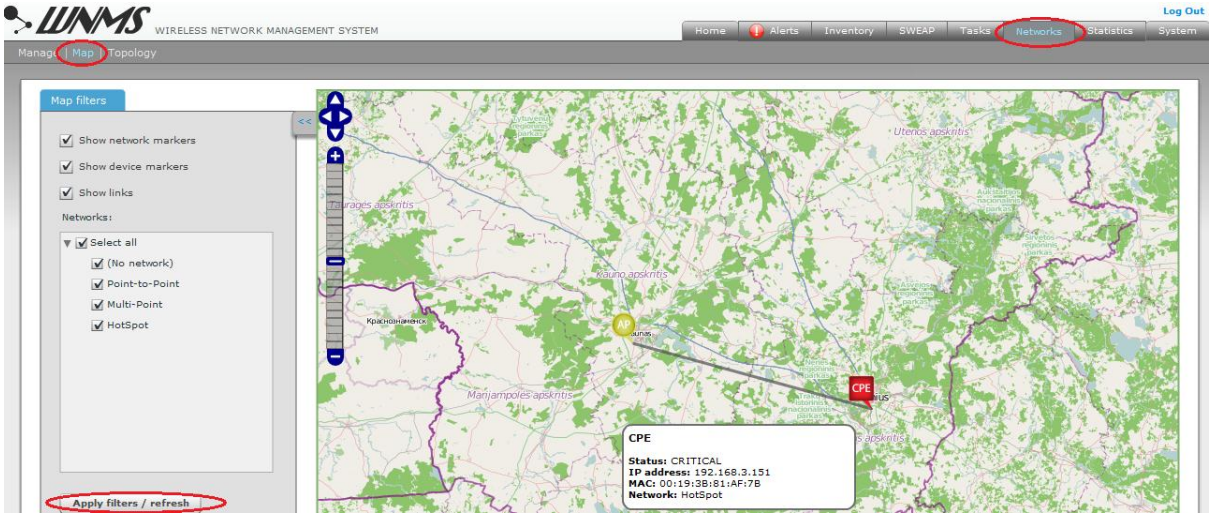


Figure 33 – Graphical Display of the Link on the Maps

The color of the device icon indicates alert state (refer to the respective section of *Alerts* for information how to setup Alert monitoring on the devices):

- Green icon means that device has no alert or has informational level alerts (active/inactive/closed).
- Yellow icon means that device has active warning level alerts or had in the past critical/warning alerts but now they are closed (not cleared) or had inactive critical/warning alerts (not cleared)
- Red icon means that device has active critical level alerts (not including inactive alerts)

Step 5. Navigate to the **Networks | Topology** menu; select network of your devices, and click **Apply filters / Refresh** button. The representation of your selected network's topology including link quality will be displayed:

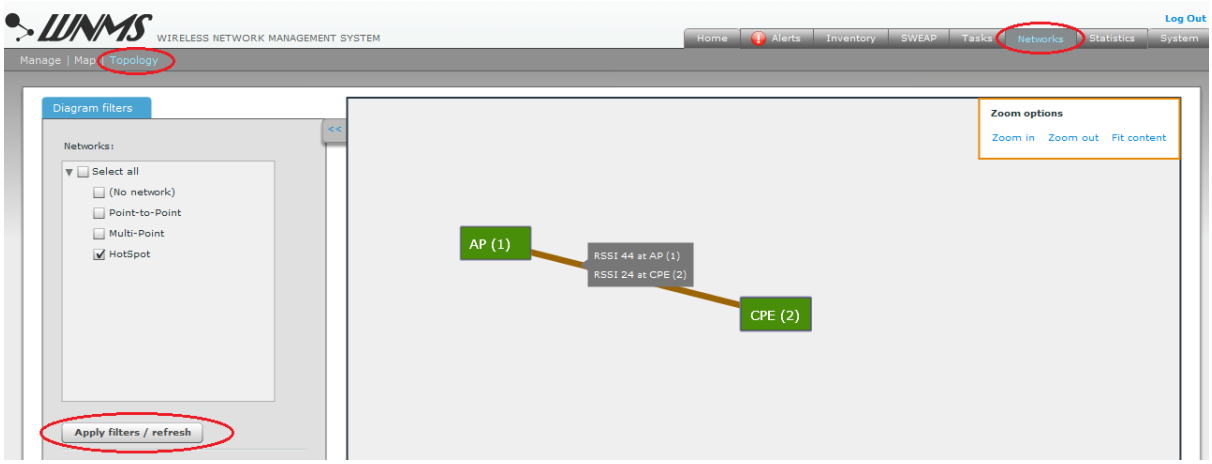


Figure 34 – Network Topology

WNMS Troubleshooting

This chapter contains information how to gather troubleshooting information about necessary component before contact support team.

Troubleshooting WNMS on Linux

WNMS processes check

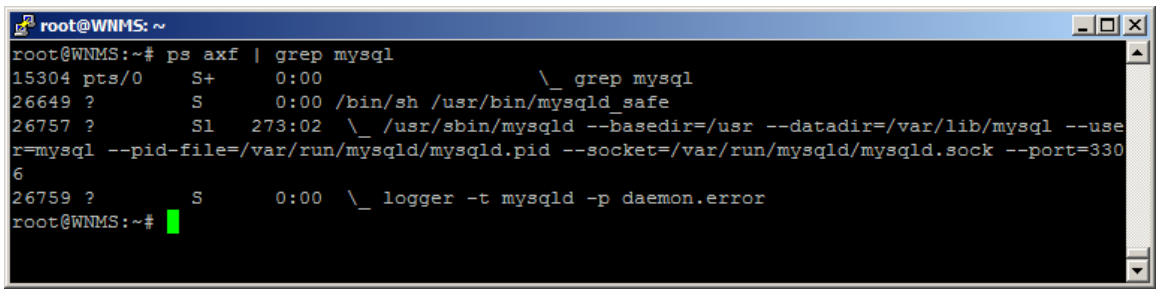
WNMS operation depends on following processes:

- MySQL database;
- Apache2 web server (collector and GUI);
- Monitoring daemon;
- WNMS-submitter daemon;
- Mail-send tool.

Login to your Linux machine console and check if these processes are running and available. The following commands are used to gather required logs for appropriate WNMS processes.

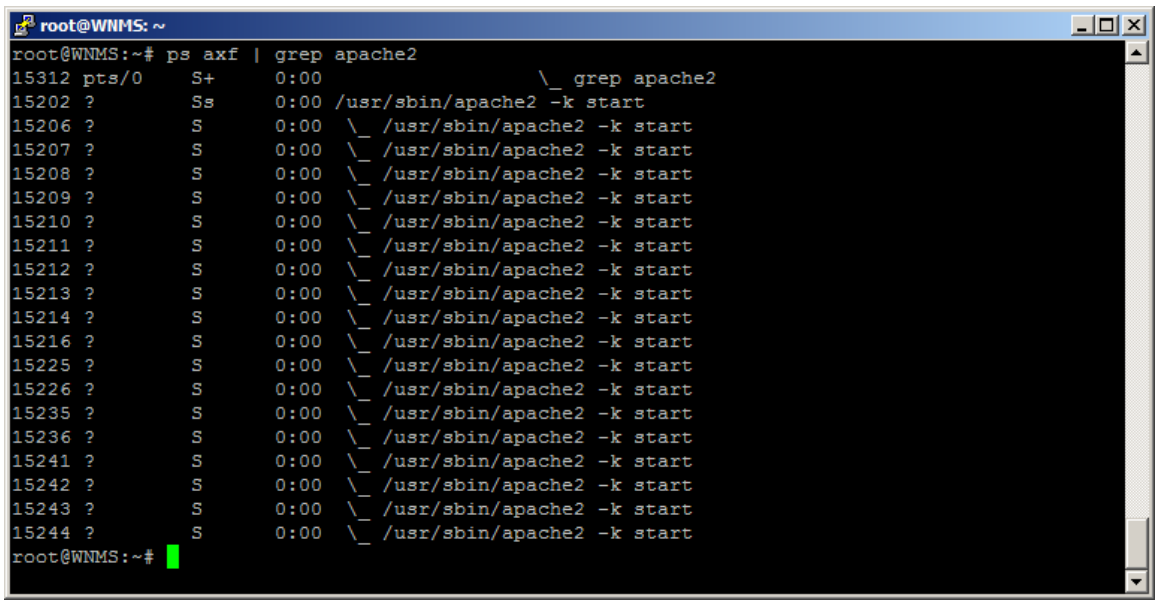
- **MySQL**: type command:

```
root@WNMS:~# ps axf | grep mysql
```



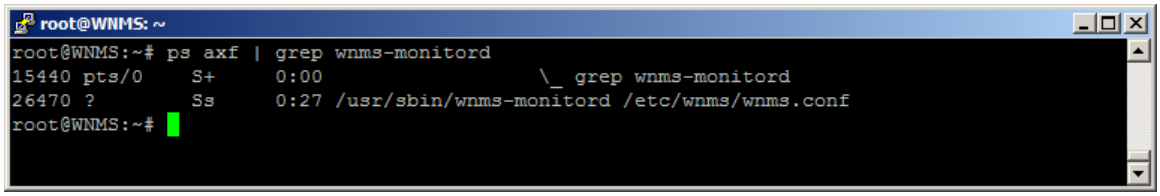
- Apache2

```
root@WNMS:~# ps axf | grep apache2
```



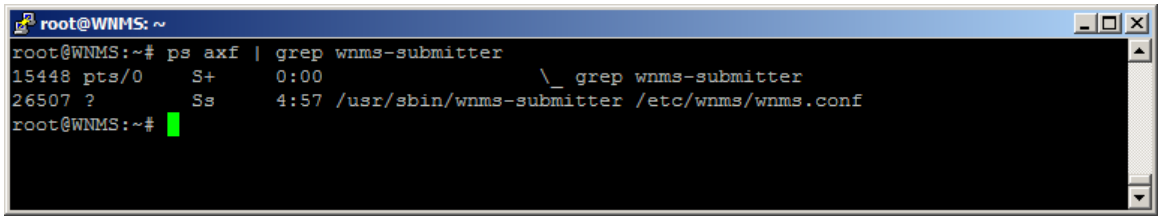
- Monitoring daemon

```
root@WNMS:~# ps axf | grep wnms-monitord
```



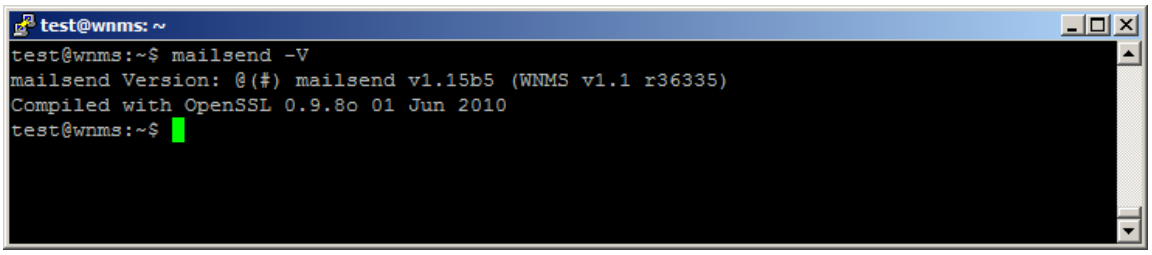
- WNMS-submitter daemon

```
root@WNMS:~# ps axf | grep wnms-submitter
```



- Mail-send tool

```
root@WNMS:~# mailsend -V
```



Version check of the WNMS components

The following commands are used to check versions of the appropriate components:

Collector version:

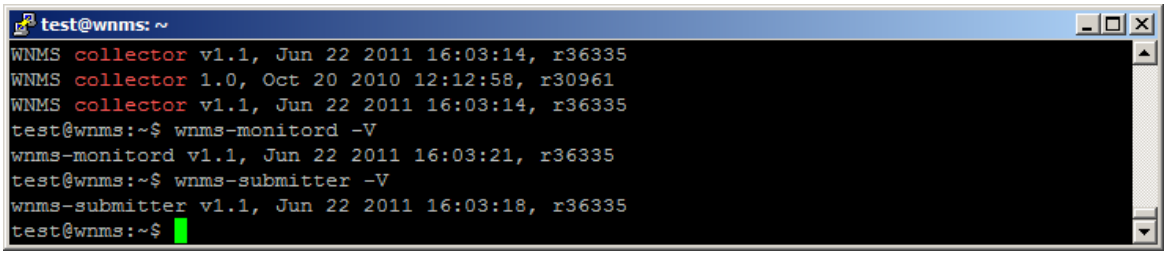
```
root@WNMS:~# cat /var/log/apache2/error.log | grep collector
```

WNMS-monitor version:

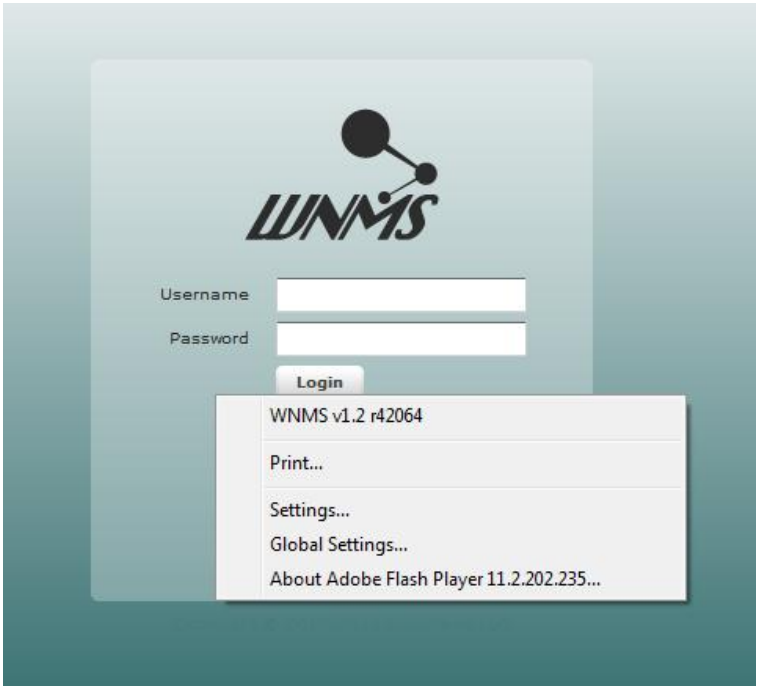
```
root@WNMS:~# wnms-monitord -V
```

WNMS-submitter version:

```
root@WNMS:~# wnms-submitter -V
```



To check **GUI version,** right mouse click on GUI (version is WNMS v1.30961 in example):



WNMS configuration files

WNMS configuration files are located at `/etc/wnms directory:`

```
root@WNMS:/etc/wnms# ls -l /etc/wnms/
-rw-r--r-- 1 root www-data 154 2010-10-20 12:13 wnms_collector.conf
-rw-r----- 1 root www-data 128 2010-11-24 11:03 wnms.conf
-rw-r--r-- 1 root root     455 2010-10-20 12:13 wnms_portal.conf
```

wnms.conf defines database type, login to database credentials, where to save heartbeats when database is unavailable and temporary file size.

```
wnmsDbType mysql
wnmsDbParams "host=127.0.0.1,user=wnms,pass=admin01,dbname=wnms_11"
wnmsQueuePath /tmp/
wnmsQueueMaxSize 10240000
```

wnms_collector.conf uses wnms.conf and additionally defines listening to heartbeats URL (/collector)

```
Include /etc/wnms/wnms.conf
<Location /collector>
                SetHandler wnms-handler
</Location>
```

wnms_portal.conf defines WNMS web content location and other PHP options.

```
Alias /wnms /usr/share/wnms-server/portal
```

```
<Directory /usr/share/wnms-server/portal>
        AllowOverride None
        Options -Indexes +FollowSymLinks
        Order allow,deny
        Allow from all

        <IfModule mod_php5.c>
                AddType application/x-httpd-php .php

                php_flag magic_quotes_gpc Off
                php_value upload_max_filesize 10M
                php_value memory_limit 32M
                php_value include_path .
        </IfModule>

        <IfModule mod_rewrite.c>
                RewriteEngine On
                RewriteBase /wnms/
                RewriteOptions Inherit



                RewriteRule ^backend/index.php/(.+)$ -
[E=DBPARAMS:127.0.0.1:wnms:unaiGi8f:wnms_11,L]
                RewriteRule ^backend/(.+)$ backend/index.php/$1 [L]
        </IfModule>
</Directory>
```

WNMS web content

WNMS web content is located at /usr/share/wnms-server/portal

```
   root@WNMS:~# ls -l /usr/share/wnms-server/portal
```

-rw-r--r-- 1 root root 8641 2011-06-22 16:04 AC_OETags.js

drwxr-xr-x 3 root root 4096 2011-08-12 10:59 backend

drwxr-xr-x 3 root root 4096 2011-08-12 10:47 com

drwxr-xr-x 2 root root 4096 2011-08-12 10:59 history

-rw-r--r-- 1 root root 4455 2011-06-22 16:04 index.html

-rw-r--r-- 1 root root 1317975 2011-06-22 16:04 nms.swf

-rw-r--r-- 1 root root 657 2011-06-22 16:04 playerProductInstall.swf

drwxr-xr-x 2 root root 4096 2011-08-12 10:59 resources

drwxr-xr-x 3 root root 4096 2011-08-12 10:59 wnms-php

WNMS GUI is made with Adobe Flex (nms.swf). PHP code (wnms-php directory) is used for communication between MySQL database and the GUI.

WNMS log files

Apache2/collector error logs:

```
root@WNMS:~# less /var/log/apache2/error.log
```

Apache2/collector access logs:

```
root@WNMS:~# less /var/log/apache2/access.log
```

Wnms-monitord logs:

```
root@WNMS:~# less /var/log/syslog | grep wnms-monitord
```

Wnms-submitter logs:

```
root@WNMS:~# less /var/log/syslog | grep wnms-submitter
```

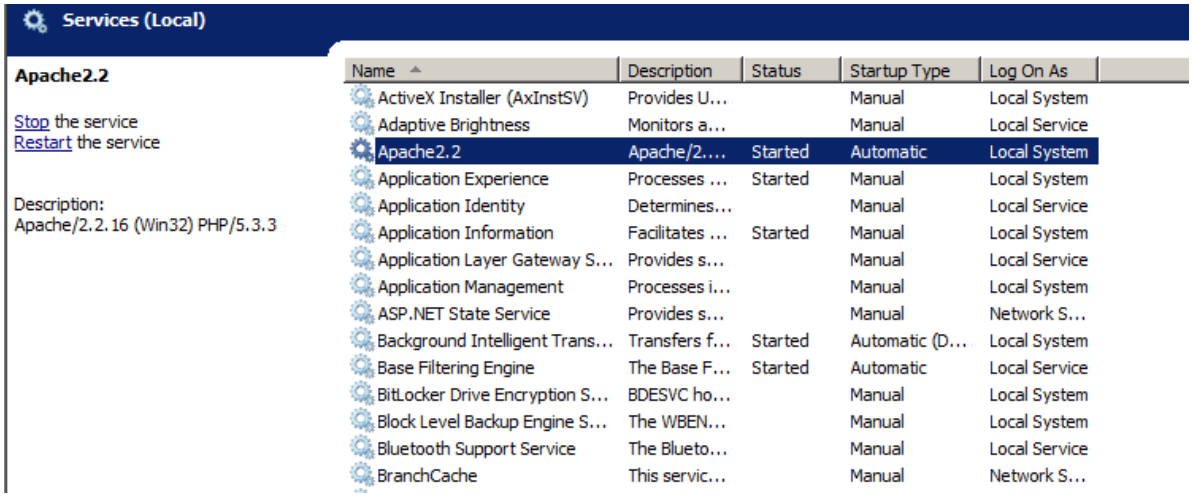
Troubleshooting WNMS on Windows

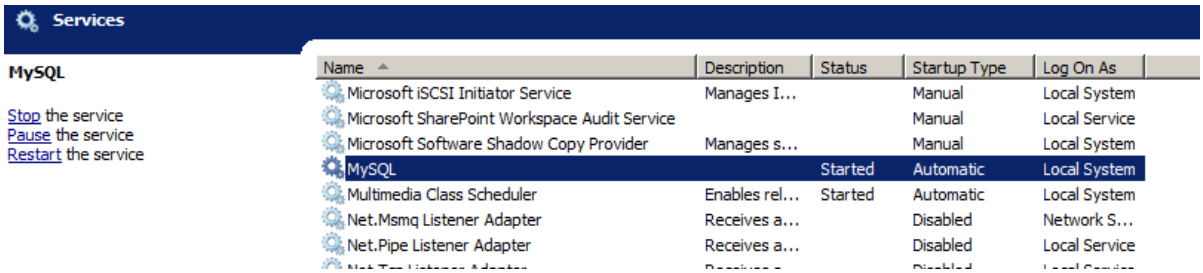
WNMS processes check

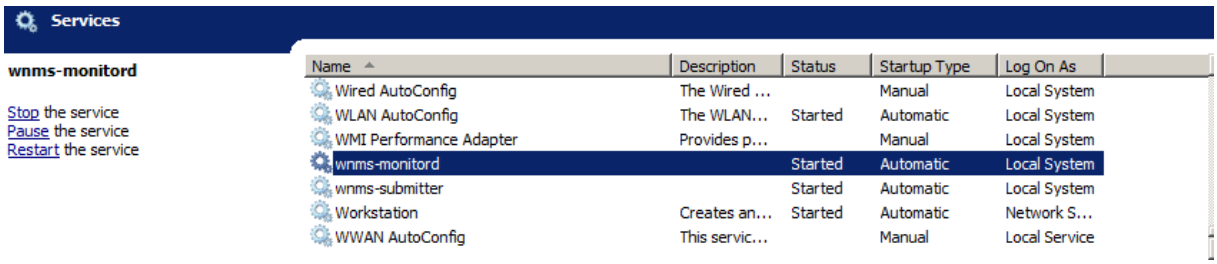
The WNMS operation depends on following processes:

- MySQL database;
- Apache2 web server (collector and GUI);
- Monitoring daemon;
- WNMS-submitter daemon;
- Mail-send tool.

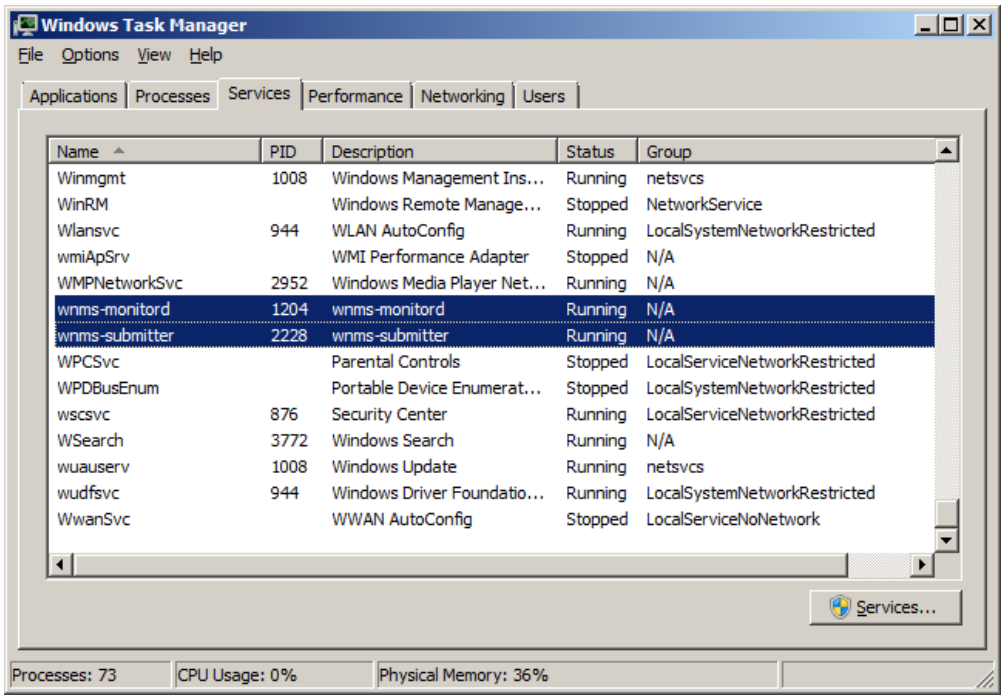
Follow the instructions to check if the appropriate WNMS processes are running. Go to **Control Panel** -> **Administrative tools** -> **Services** and check if Apache2.2, MySQL, wnms-monitord and wnms-submitter have status "**Started**".



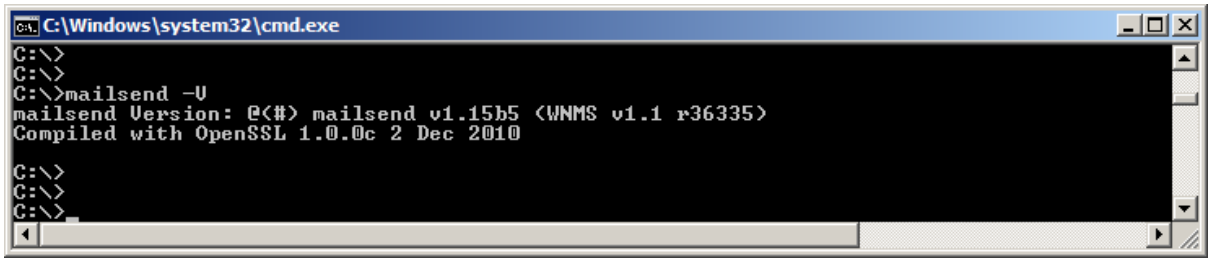




If everything works well, these WNMS processes can be seen on Windows Task Manager, Services section:



Go to Start, run “cmd” and check if mailsend tool is available (`mailsend -V`)



WNMS components version check

Go to Start, run “cmd” and submit the following command for version checking:

Collector version:

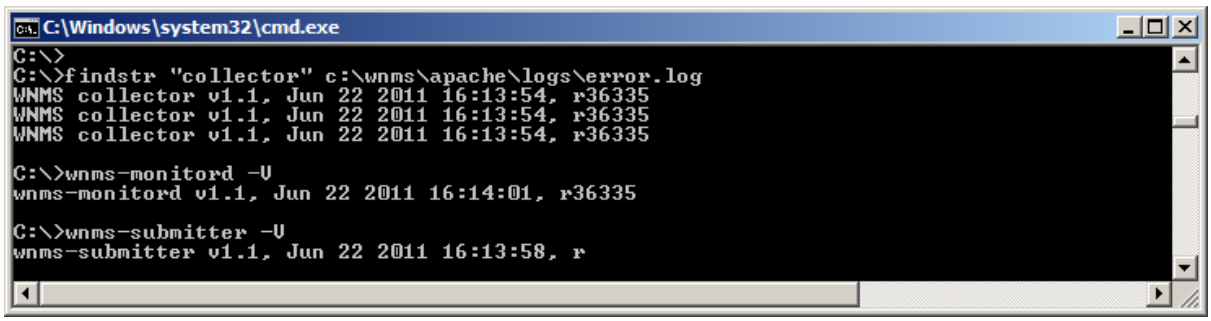
```
C:\>findstr "collector" c:\wnms\apache\logs\error.log
```

WNMS-monitor version:

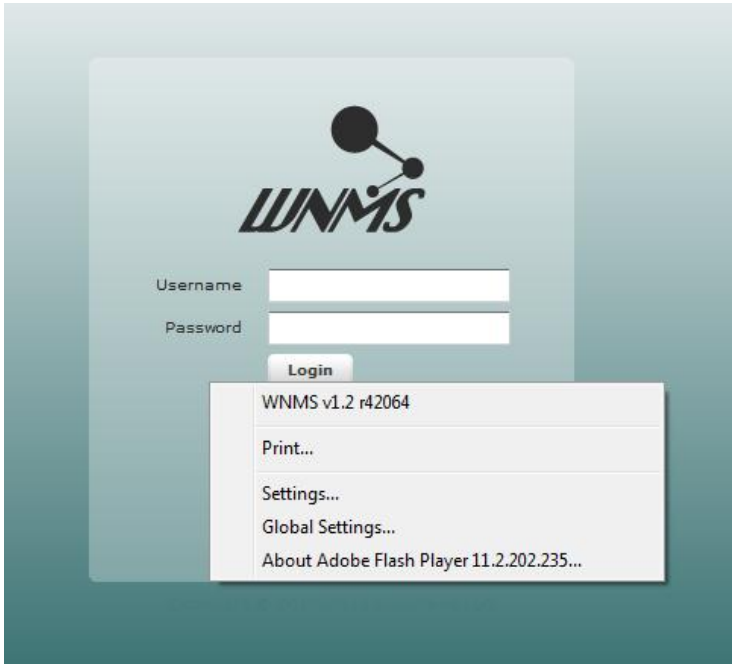
```
C:\>wnms-monitord -V
```

WNMS-submitter version:

```
C:\>wnms-submitter -V
```



To check **GUI version,** right mouse click on GUI (version is WNMS v1.30961 in example):



WNMS configuration file

Default WNMS installation folder is `C:\>wnms.`

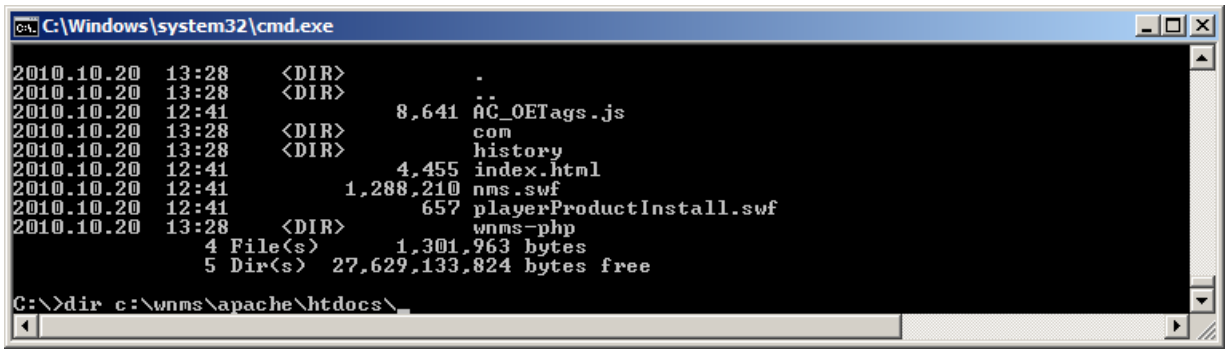
WNMS configuration file that is used for **collector**, **wnms-monitord** and **wnms-submitter** components is located here:

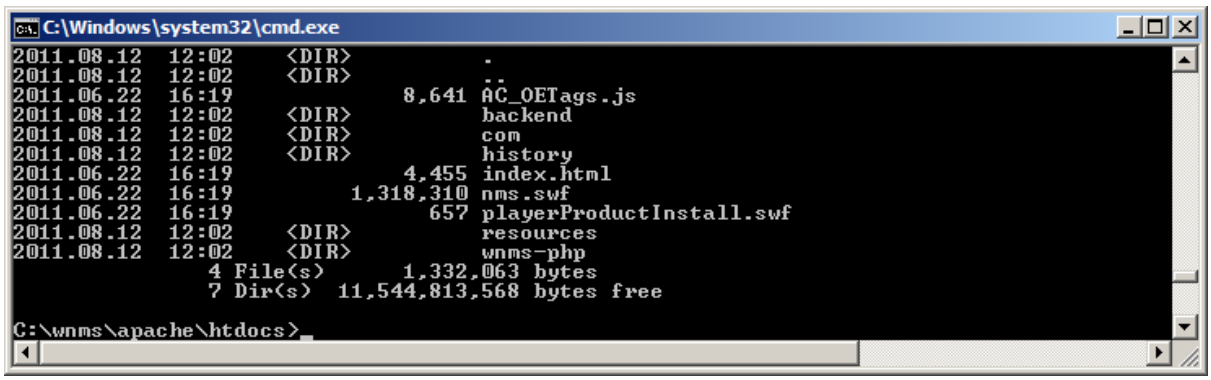
```
C:\>wnms\apache\conf\extra>httpd-wnms.conf:
LoadModule wnms_module C:/wnms/wnms/mod_wnms.so
wnmsDbType mysql
wnmsDbParams "host=127.0.0.1,user=wnms,pass=admin01,dbname=wnms_11"
wnmsQueuePath C:/wnms/tmp
wnmsQueueMaxSize 10240000

<Location /collector>
        SetHandler wnms-handler
</Location
```

This file defines WNMS collector module path, connection to database credentials, place where heartbeats are saved when database is unavailable, size of temporary heartbeats file and URL collector listens to heartbeats.

WNMS web content

WNMS web content is located at `C:\wnms\apache\htdocs`





WNMS GUI is made with Adobe Flex (nms.swf). PHP code (wnms-php directory) is used for communication between MySQL database and the GUI.

WNMS log files

The WNMS log files are located in the following directories, and can be opened with any text editor (eg. Notepad, WordPad):

Apache2/collector error logs:

`C:\wnms\apache\logs>error.log`

Apache2/collector access logs:

`C:\wnms-folder\apache\logs>access.log`

Wnms-monitord logs:

`C:\wnms\wnms\logs>wnms-monitord.log`

Wnms-submitter logs:

`C:\wnms\wnms\logs>wnms-submitter.log`

WNMS agent troubleshooting

WNMS agent runs on the devices and depends on following processes:

- Alert daemon (alertd)
- SNMP daemon (snmpd)

WNMS agent basically performs communication task between the collector and the device. The alert daemon performs all alert functionality, whereas the SNMP daemon is required for various statistical data getting from the device.

Follow the instructions how to check the running processes. Login to the device via SSH, then type "**shell**" and execute following commands for the appropriate process:

WNMS agent:

```
# ps axf | grep wnms
```

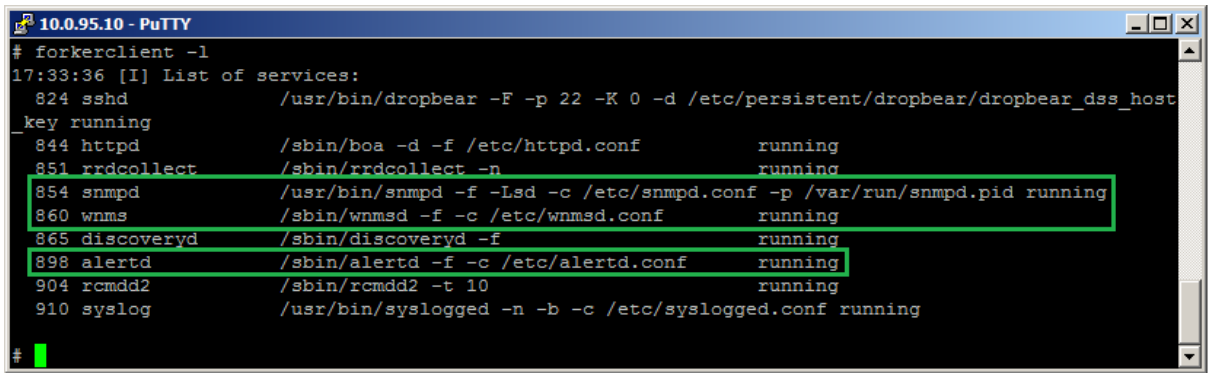
Alert daemon:

```
# ps axf | grep alertd
```

SNMP daemon

```
# ps axf | grep snmpd
```

All these processes shall also be included in the **forkerclient**. To view if the appropriate processes are included into the forkerclient, type the command `forkerclient -l` in the shell:



Check log files

WNMS agent logs:

```
# cat /var/log/messages | grep wnmsd
```

Alert daemon logs:

```
# cat /var/log/messages | grep alertd
```

Check WNMS heartbeats

It is very important to check when the last heartbeat was sent to the collector. Last heartbeat from the agent and last heartbeat reply from the collector are located at `/tmp/wnms` directory.

Type command:

```
# ls -l /tmp/wnms/
-rw-------  1 admin    admin      1345 Jan 16 13:47 last-heartbeat
-rw-------  1 admin    admin      2022 Jan 16 13:47 last-heartbeat-reply
```

If there is no information about the last heartbeat on the device, this means that WNMS server is unreachable.

To view content of the last heartbeat, type command "`cat /tmp/wnms/last-heartbeat`" and "`cat /tmp/wnms/last-heartbeat-reply`":

```
# cat /tmp/wnms/last-heartbeat
<?xml version="1.0" encoding="UTF-8"?>
<heartbeat version="2">
        <counter>4360</counter>
        <mac-address>00:19:3B:81:5C:06</mac-address>
        <ip-address>10.0.95.10</ip-address>
        <serial-number>0101102900000112</serial-number>
        <device-name>Test1</device-name>
        <firmware-revision>LIGO-PTP.FWBD-0100.v6.80-
DEVEL.rt2880.LIGO.PTP.en_US.31823.101206.084706</firmware-revision>
        <config-MD5>3678119ACB8444556C0DABF0E44E30F2</config-MD5>
        <coordinates longitude="25.201645" latitude="54.432464" />
        <topology>
                <interface type="ethernet" name="eth0" mac="00:19:3B:81:5C:06">
                </interface>
                <interface type="wireless" name="ra0" mac="00:19:3B:81:5C:06">
                        <data type="rssi">37</data>
                        <peers>
                                <peer mac="00:19:3b:81:5c:08"/>
                        </peers>
                </interface>
                <interface type="wireless" name="wds0" mac="00:19:3B:81:5C:06">
                        <data type="rssi">-4</data>
                        <peers>
                                <peer mac="00:19:3b:81:5c:08"/>
                        </peers>
                </interface>
        </topology>
        <alarms>
        </alarms>
        <statistics>
                <stat id="1">-57</stat>
                <stat id="2">-95</stat>
                <stat id="3">25942425</stat>
                <stat id="4">5260</stat>
                <stat id="5">0.000000</stat>
                <stat id="8">1</stat>
                <stat id="9">93</stat>
```

```
                <stat id="10">6448</stat>
                <stat id="13">503871693</stat>
                <stat id="14">141930231</stat>
                <stat id="15">3769</stat>
                <stat id="16">0</stat>
        </statistics>
</heartbeat>



# cat /tmp/wnms/last-heartbeat-reply
HTTP/1.1 200 OK
Date: Fri, 10 Dec 2010 11:03:35 GMT
Server: Apache/2.2.14 (Ubuntu)
Content-Length: 1867
Connection: close
Content-Type: text/plain
<?xml version="1.0" encoding="UTF-8"?>
<heartbeat-reply version="2">
  <heartbeat-interval>60</heartbeat-interval>
  <requested-statistics>
       <stat id="1" oid=".1.3.6.1.4.1.32750.3.5.1.2.1.1.14.3" desc="Signal level
(mimo)" />
       <stat id="2" oid=".1.3.6.1.4.1.32750.3.5.1.2.1.1.15.3" desc="Noise level
(mimo)" />
       <stat id="3" oid=".1.3.6.1.2.1.1.3.0" desc="Uptime" />
       <stat id="4" oid=".1.3.6.1.4.1.32750.3.5.1.2.1.1.7.3" desc="Frequency
(mimo)" />
       <stat id="5" oid=".1.3.6.1.4.1.2021.10.1.6.1" desc="CPU load" />
       <stat id="8" oid=".1.3.6.1.4.1.32750.3.5.1.2.1.1.16.3" desc="Connected radio
peers (mimo)" />
       <stat id="9" oid=".1.3.6.1.6.3.10.2.1.2.0" desc="SNMP-Engine-Boots" />
       <stat id="10" oid=".1.3.6.1.4.1.2021.4.11.0" desc="Free memory" />
       <stat id="13" oid=".1.3.6.1.2.1.2.2.1.10.$(eth0)" desc="Input bytes
(ethernet)" />
       <stat id="14" oid=".1.3.6.1.2.1.2.2.1.16.$(eth0)" desc="Output bytes
(ethernet)" />
       <stat id="15" oid=".1.3.6.1.4.1.32750.3.8.1.3.1.1.17.3.0" desc="TX retries
(mimo)" />
       <stat id="16" oid=".1.3.6.1.4.1.32750.3.8.1.3.1.1.37.3.0" desc="RX drops
(mimo)" />
      </requested-statistics>
      <requested-alarms>
              <alarm id="1" oid="" name="etherstatus" desc="" threshold="1"
op="equal"/>
              <alarm id="2" oid="" name="radiostatus" desc="" threshold="1"
op="equal"/>
```

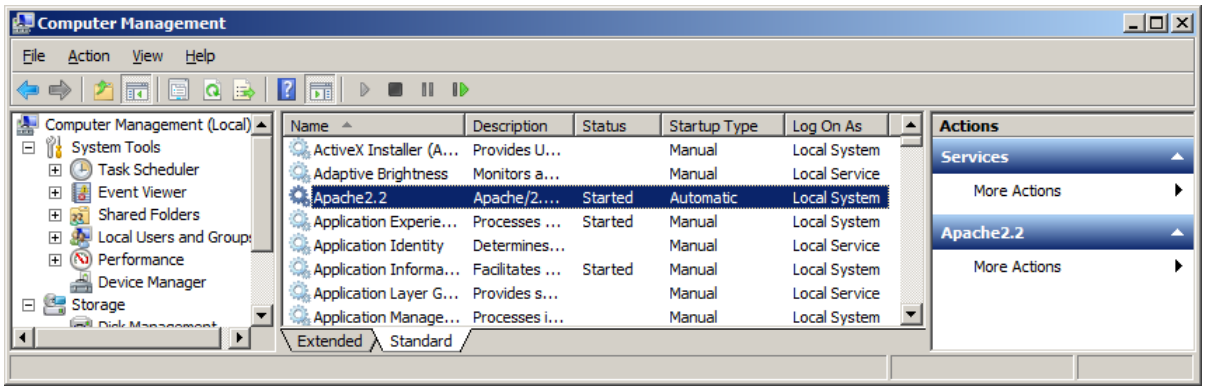
```
            <alarm id="3" oid="" name="up_and_down" desc="" threshold="1"
op="equal"/>
            <alarm id="4" oid="" name="freqchange" desc="" threshold="1"
op="equal"/>
            <alarm id="5" oid="" name="reboot" desc="" threshold="1" op="equal"/>
            <alarm id="7" oid="" name="noise" desc="" threshold="-80"
op="above"/>
            <alarm id="8" oid="" name="radiopeercount" desc="" threshold="1"
op="above"/>
            <alarm id="11" oid="" name="rxdrop_pct" desc="" threshold="5"
op="above"/>
            <alarm id="13" oid="" name="rssi" desc="" threshold="20" op="below"/>
      </requested-alarms>
</heartbeat-reply>
```

Frequently Asked Questions

Can’t access WNMS Web management on Windows.

Question: Impossible to load WNMS web management interface on Windows OS.

Answer: Check if Apache service is running**. Go to Control Panel → Administrative Tools → Services** and check status of Apache service:



If Apache is not started, check logs at **Event viewer → Windows logs → Application** and try to find out the reason why this service is not started.

Forgot password of WNMS Web management

Q: how to reset administrator’s password of WNMS web management?

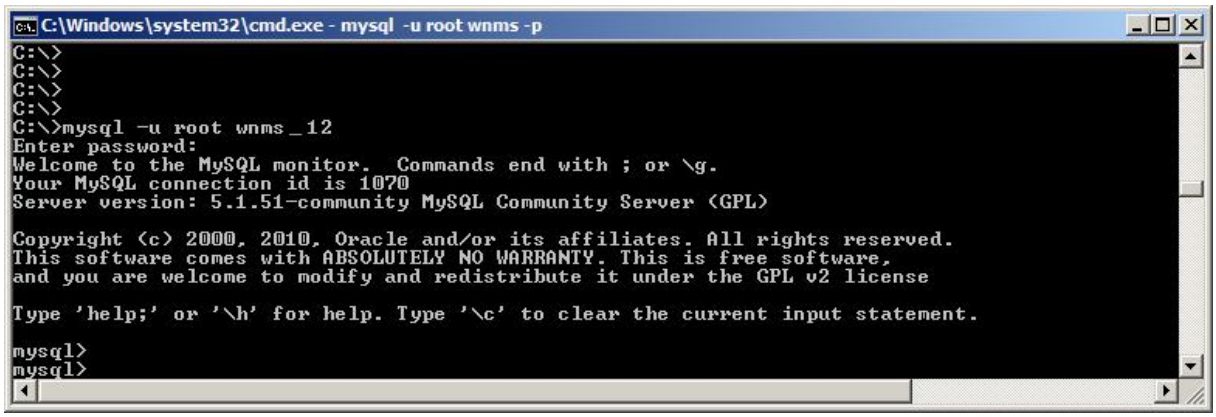
A: the procedure of web management password reset differs dependently on OS where the WNMS was installed.

Reset password on Windows OS

Step 1. Start command prompt on WNMS server, type:

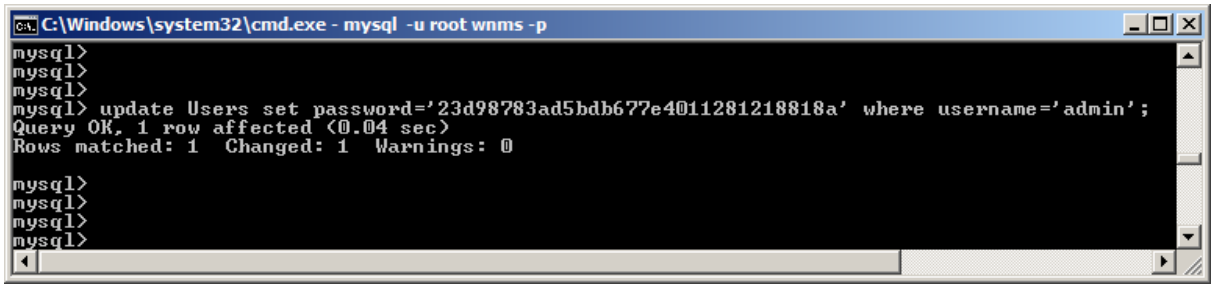
```
mysql -u root wnms_12 -p
```

and press Enter twice:



Step 2. To set default password (admin01) for admin user, type encrypted default password:

```
update Users set password='23d98783ad5bdb677e4011281218818a'
where username='admin';
```



If username is other, type it in the command, e.g ...where username='test';

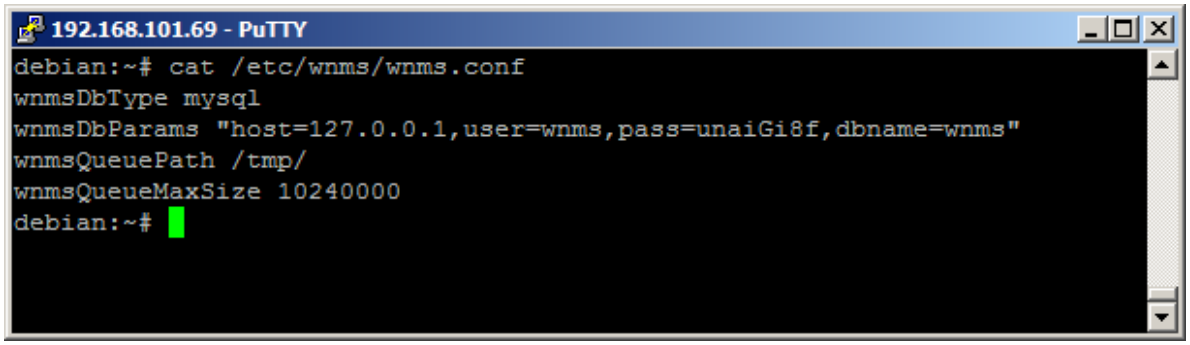
Reset password on Linux OS

Step 1. If MySQL root password is known, type the following command in server terminal

```
#  mysql –u root wnms_12 –p
```

If MySQL root password is not known, find out wnms user password:

```
# cat /etc/wnms/wnms.conf
```

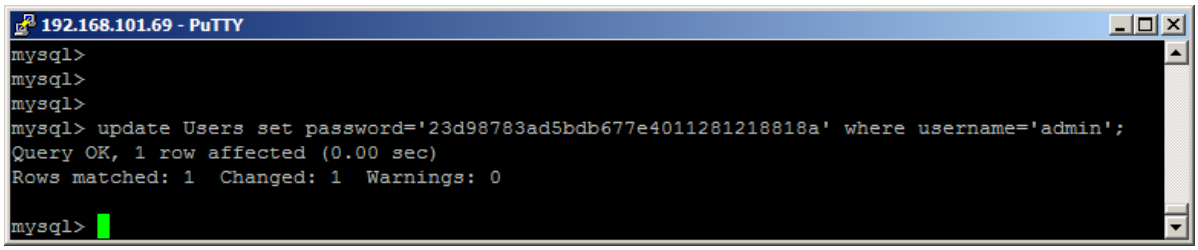


Step 2. Then access MySQL

```
# mysql -u wnms wnms -p'unaiGi8f'
```

Step 3. Set admin user password to default (admin01)

```
update Users set password='23d98783ad5bdb677e4011281218818a'
where username='admin';
```



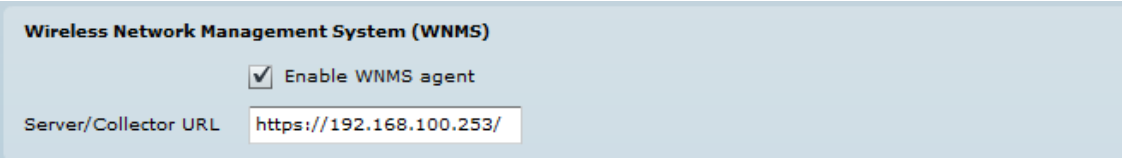
Devices do not appear on WNMS server.

Q: devices don't appear on WNMS server.

A: there can be several reasons why devices still don't appear on WNMS server. Please check the following options:

- It takes 5 minutes for device to appear on WNMS server, as default heartbeat interval (device communication with WNMS server) is 5min.

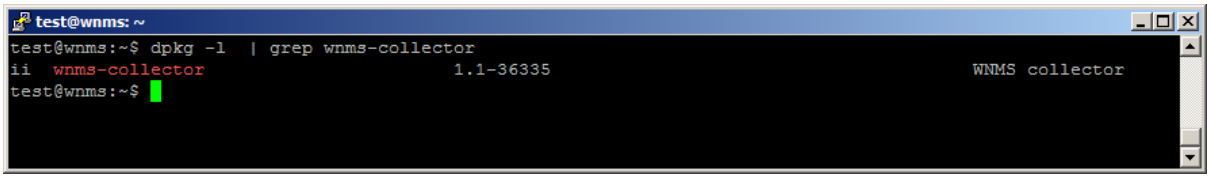
- Check if WNMS agent is enabled and correct URL is set on device web management interface:



- Check network settings and firewall: WNMS server uses HTTP (TCP 80) port, therefore there is possibility that network settings are misconfigured and devices can't reach WNMS server.

- Check if WNMS collector package is installed successfully (only on Linux OS), type command:

```
# dpkg -l | grep wnms-collector
```

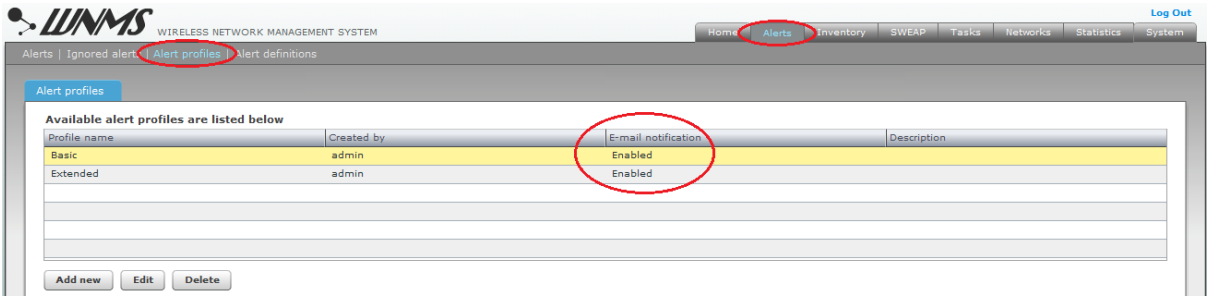


Not getting emails on alert events

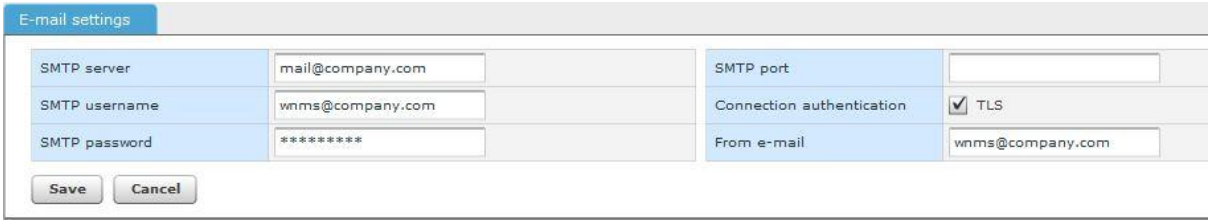
Q: Can see alerts, but don't get an email notifications on alert events. What is a problem?

A: Follow the steps to verify if the e-mail notification was configured properly:

Step 1. First check if correct email is defined in **Alerts | Alert profile** settings:



Step 2. Then check does SMTP settings at **System | System settings | Email settings** are provided correctly. Check connection authentication - if SNMP server requires SSL/TLS, select "TLS" option:

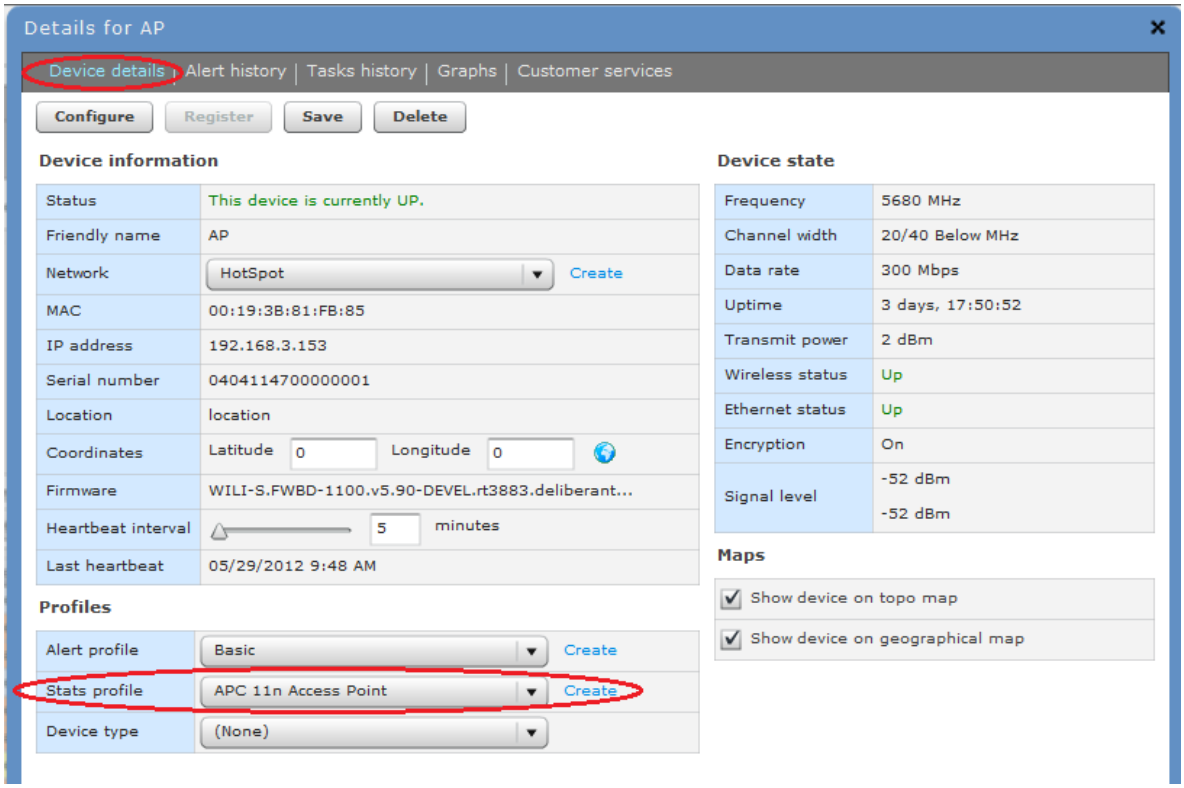


No graphs are displayed

Q: When I load **Device Details** window and navigate to the Graph section, I can't see any graphs at all.

A: There can be several reasons why there are no graphs displayed:

- First load **Device Details** window and check if the **Statistics profile** is assigned to the device. If no statistics profile assigned, then device will not gather statistical data therefore no graphs will be available to display:



- Check if proper statistics profile is assigned to the devices. Load **Device Details** window and check if the statistics profile match the device type (for example for APC device only APC<…> statistics profiles can be assigned, do not use PTP or PTP MiMo statistics).

- Wait at least 20 minutes if the default heartbeat interval (5min) is specified on device – it takes time for WNMS to gather enough data to draw a graph.

Some of graphs are empty

Q: I have assigned a statistics profile, but some of the graphs are empty.

A: There can be several reasons why some of the graphs are not displayed:

- This issue can happen with APC device, that has "APC 11n all products" statistics profile assigned. This statistics profile includes statistics additionally for one virtual radio (VAP), therefore if the device has no VAP created, several graphs will be displayed empty as there won't be any statistical data to display.
- Also if graphs are added as "bulk" (**Statistics | Graphical reports, Add graphs**), check does all selected statistics definitions are proper for the particular type of devices (for example if you created graph for APC device and included "PTP TX retries" statistics definition, sure such graph will not be drawn).

A new task was not performed – still pending status

Q: newly created task “reboot” was configured to execute “now” but device is still not rebooted, the task still has “pending” status.

A: default heartbeat interval (communication between device and WNMS) is 5 minutes, according this the task that was configured to be executed “now” will be performed as soon as the heartbeat-reply will reach the device.

There is possibility to change heartbeat interval (1-120 minutes) on **Inventory | Device Details**.

What is the maximum number of devices supported by WNMS?

A: there is no hard limitation of monitored devices. Devices amount depends on server performance, configured heartbeat interval, and network topology. Recommended device amount could be about five thousands.

When system cleanup should be performed?

A: it is recommended to perform System cleanup (**System | System Cleanup** menu on Web management interface) once per six months.

All collected data will be removed permanently, so perform system cleanup only if old data is not necessary.

Index