

INFOWATCH

# InfoWatch Traffic Monitor 6.1

Installation Guide

**InfoWatch Traffic Monitor 6.1**

# Installation Guide

© AO “InfoWatch”

Tel/Fax +7 (495) 229-00-22

http://www.infowatch.com

Revision date: 2016-05-24

TABLE OF CONTENTS

**1 INTRODUCTION ..... 4**

1.1 WHO SHOULD READ THIS GUIDE ..... 4
1.2 SET OF DOCUMENTS ..... 4
1.3 TECHNICAL SUPPORT ..... 4

**2 GETTING READY TO INSTALL ..... 6**

2.1 SYSTEM DEPLOYMENT SCHEMES AND INSTALLATION TYPES ..... 6
2.2 HARDWARE AND SOFTWARE REQUIREMENTS ..... 8

**3 INSTALLING THE SYSTEM ..... 12**

3.1 GENERAL INFORMATION ON INSTALLATION STEPS ..... 14
*3.1.1 Start Window ..... 14*
*3.1.2 Selecting the Database ..... 15*
*3.1.3 Selecting the Installation Mode ..... 16*
*3.1.4 Choosing a Time Zone ..... 17*
*3.1.5 Setting Password for System Superuser ..... 18*
*3.1.6 Choosing a Disk Partitioning Method ..... 18*
*3.1.7 Network Settings ..... 22*
*3.1.8 Configuring Time Synchronization (NTP-server) ..... 25*
*3.1.9 Localization Setting ..... 26*
*3.1.10 Configuring the Automatic Event Deletion from the Database ..... 28*
*3.1.11 Completing the Installation ..... 29*
3.2 ALL-IN-ONE INSTALLATION MODE OF TM ENTERPRISE AND TM STANDARD ..... 30
3.3 DISTRIBUTED INSTALLATION OF TM ENTERPRISE ..... 36
*3.3.1 Installing Database (TM DB Server) ..... 36*
*3.3.2 Installing Traffic Monitor Server (TME Node Server) ..... 40*
3.4 INSTALLATION OF TM APPLIANCE STANDARD AND TM APPLIANCE ENTERPRISE ..... 42
3.5 INSTALLING THE CRAWLER SUBSYSTEM ..... 45
3.6 PRE-INSTALLED SERVER SETTINGS ..... 49

**4 UPDATING THE SYSTEM ..... 51**

4.1 UPDATING RHEL AND IWTM PACKAGES ..... 52
4.2 UPDATING THE ORACLE DATABASE SCHEMA ..... 53
4.3 UPDATING THE POSTGRESQL DATABASE SCHEMA ..... 54

**5 UNINSTALLING THE SYSTEM ..... 56**

5.1 DELETING THE DATABASE SCHEME ..... 56
5.2 CRAWLER ..... 58

**6 APPENDIX A. USERNAME AND PASSWORD RECOMMENDATIONS ..... 59**

**7 APPENDIX B. LICENSES FOR THIRD-PARTY TECHNOLOGIES ..... 61**

# 1 INTRODUCTION

This guide contains information on installation, configuration, update and uninstallation of InfoWatch Traffic Monitor (IW TM).

Besides, the document describes the deployment of the System in the Appliance mode: IW TM Appliance is designed for the easiest integration of InfoWatch Traffic Monitor into an existing infrastructure.

## 1.1 Who Should Read this Guide

This document is intended for InfoWatch company technical support service and support engineers of InfoWatch partner companies.

## 1.2 Set of Documents

For more information see the following documents:

- «*InfoWatch Traffic Monitor. User Guide*».

The document describes operation with InfoWatch Traffic Monitor: configuration setting, data export/import, creating policies for objects processing.

- «*InfoWatch Traffic Monitor. Administration Guide*».

Contains information on System administration (database, server-end).

- *«InfoWatch Device Monitor. User Guide»*

Contains a description of the InfoWatch Device Monitor system operation principles as well as instructions on installation, configuration of a system, and system maintenance.

## 1.3 Technical Support

If you cannot resolve issues which arise when using the System or have questions regarding the use of the System, you can contact the Technical Support Service:

- If you purchased the product from an InfoWatch partner, contact the Technical Support Service of this partner company.
- If you purchased the product directly from InfoWatch, you can contact our Technical Support Service at support@infowatch.com.

Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+3, summer GMT+4), except weekends and public holidays in Russian Federation.

You can also visit online support at our website at: http://infowatch.com/support.

Before contacting the Technical Support Service, please refer to the Knowledge Base at our web-site: https://kb.infowatch.com/. The knowledge base may already contain the answer to your question or a description of the problem you are having.

# 2 GETTING READY TO INSTALL

In this chapter, you can find information on:

- System deployment schemes and supported installation types;
- software and hardware requirements.

## 2.1 System Deployment Schemes and Installation Types

InfoWatch Traffic Monitor features depend on the installation mode (TM / TM Appliance), the database in use (Oracle / PostgreSQL), and the edition (Standard / Enterprise).

The following typical solutions can be:

- **InfoWatch Traffic Monitor Enterprise Appliance** is an integrated hardware and software solution for companies from 400 up to 1000 employees. Provides a full range of Traffic Monitor Enterprise functions on the single server. See details at the official site of the Company: http://infowatch.com/products/traffic_monitor_enterprise/appliance.
- **InfoWatch Traffic Monitor Standard Appliance** is an integrated hardware and software solution for companies up to 300 employees. See details at the official site of the Company: http://www.infowatch.ru/products/traffic_monitor_standard/appliance.
- **InfoWatch Traffic Monitor Standard** is a solution for companies up to 300 employees. It has a set of restrictions as compared to Enterprise version (see details in the table below and http://infowatch.com/products/traffic_monitor_standard/difference). The solution is deployed on a single server.
- **InfoWatch Traffic Monitor Enterprise** is an integrated scalable solution with a flexible configuration of components. The most extensive configuration can include the following components:
    - **Traffic Monitor Server** enables operation of interceptors (IW_SNIFFER, IW_ICAP and IW_SMTPD), the analysis subsystem, and the Policy Applying subsystem. In some cases, several Traffic Monitor servers should be used: this enables more efficient operation of loaded processes. Besides, you should take into account that some processes should run on one server only (see details in "Checking Process Autorun" article of the Administration Guide).
    - **Database** is Oracle or PostgreSQL DBMS server. You should not install or run applications (especially server ones) on it or use this computer as a file server.
    - **Device Monitor** is an interception module designed as server part with Management console and Agents deployed to computers and mobile devices of a company. See description of this module in "InfoWatch Device Monitor. User Guide".
    - **Crawler** is an interception module designed as server and scanner services.
    - **Connectors** are a set of interception modules for integration with external systems.

- **Management console** is a web interface for System managing designed as a set of processes which should run at the only one Traffic Monitor server (see details in "Checking Process Autorun" article of the Administration Guide).

The following table describes the functional difference between System editions depending on the database in use.

| Feature | TM Enterprise | | TM Standard | |
|---|---|---|---|---|
| | TM Enterprise Oracle | TM Enterprise PostgreSQL | TM Standard Oracle | TM Standard PostgreSQL |
| Storage period of intercepted data | Limited by storage size only | | Limited by 200 GB and depends on the volume of outgoing traffic generated by users | Limited by storage size only |
| Computers control | Control of using removable devices, communication ports, print control | | Optional (the availability of InfoWatch Device Monitor computer control module using depends on data size and required storage period) | |
| Scalability | The solution can be adapted for servicing a large number of employees (tens of thousands) scaling the company growth. Can be used for geographically-distributed company branches connected by any communication channels | | Designed for companies with up to 300 employees | |
| Blocking traffic transfer when the violation was found | Yes | | Optional (implementation is held by certified engineers only) | |
| Integration scheme | Several options available: "in-line" integration, ICAP support, intercepting the traffic copy (SPAN, port mirroring, etc.) | | Operating in traffic copy mode ("in-line" integration is optional) | |

There are following installation types:

- *All-in-one Standard* – all the System components (together with Oracle Standard or PostgreSQL DBMS) are installed on the same server. This installation type is used if, with respect to the assumed load, the server has resources for DBMS and TM services.
- *All-in-one Enterprise* – all the System components (together with Oracle Enterprise or PostgreSQL DBMS) are installed on the same server. This installation type is used if, with respect to the assumed load, the server has resources for DBMS and TM services.
- *Traffic Monitor Server* + *Database* – Traffic Monitor Server and DBMS (Oracle Enterprise or PostgreSQL) are installed on different computers. This installation type is used if, with respect to the assumed load, DBMS and TM services cannot efficiently operate on the same server.

**Warning!**

After installation, the Administrator configures the System depending on implementation purposes (see "*InfoWatch Traffic Monitor. Administration Guide*", "Configuring the System after Installation").

## 2.2 Hardware and Software Requirements

For the Traffic Monitor Server, hardware requirements are defined basing on the deployment scheme, the estimated load on the System and parameters of the network where the System is installed. Therefore, equipment specification is determined individually in each case.

Variants of the System deployment schemes are described in "System Deployment Schemes and Installation Types". According to the article, there can be following elements to install:

- **Server for "All-in-one" installation** is used for:
  - TM Enterprise Appliance – requirements are specified on the official site: http://infowatch.com/products/traffic_monitor_enterprise/appliance
  - TM Standard Appliance – requirements are specified on the official site: http://www.infowatch.ru/products/traffic_monitor_standard/appliance
  - TM Standard – *See requirements below.*
  - TM Enterprise – installing the Enterprise solution in "All-in-one" mode is not recommended but possible. *See requirements for standalone TM Enterprise server.*
- **Traffic Monitor Server** – standalone server or cluster of TM Enterprise servers. *See requirements below.*
- **Database Server** – server for Oracle or PostgreSQL DBMS. You should not install or run applications (especially server ones) on it or use this computer as a file server. *See requirements below.*
- **Crawler Server and Crawler Scanner** – Wiindows services. *See requirements below .*
- **Connectors** – their requirements are listed in the documentation supplied with connectors software.
- **Device Monitor Server and Device Monitor Agents** – their requirements are listed in «*InfoWatch Device Monitor. User Guide*» supplied with the software.
- **Management Console** is automatically installed together with the Traffic Monitor Server and do not impose any additional hardware or software requirements to the server. To have an access to the Management Console you should just use Google Chrome browser v. 40 or higher.

The Traffic Monitor Server hardware and software requirements are varied in a great range. So the minimal configuration supposes following constraints:

- OCR is disabled for all interceptors;
- server do not accept data from Device Monitor and Crawler.

Significant difference in the load on certain interception channel can also influence on the number and role of Traffic Monitor Servers: for example, the efficient processing of traffic both from Device Monitor and Crawler you need to dedicate a special server for **iw_expressd** process.

Estimated minimal software and hardware requirements are listed in the following table. We strongly recommend you to make a detailed configuration computation with assistance of InfoWatch experts of specialists of partner company from which you have purchase the product.

| Traffic Monitor element | | Hard disk | **Processor** | **RAM** | Software | Additional requirements |
|---|---|---|---|---|---|---|
| TM Standard server | | About 300 GB: DB takes up to 200 GB and 100 GB for other components | 2CPU 6xC, 2,6 Ghz | 16 GB | No requirements: the kickstart installator formats the hard drive and installs all required software. | The Traffic Monitor server can use interceptors which raise additional requirements:<br>• **iw_sniffer** can get a traffic copy from swith with SPAN / Port Mirroring function (Cisco Catalyst 2960 Series is recommended) with port configured for TRx mode (BOTH - receiving and sending in the same connection).<br>• **iw_icap** handles ICAP client built in any proxy server confirming RFC 3507 standard (for example SQUID 3.2.1 or higher, Cisco IronPort S10 and Blue Coat SG Series). Please consult InfoWatch support service before using certain model to confirm the compatibility with IW ICAP module. The proxy server should contain ICAP license; enabling ICAP support is performed according to support documentation of certain proxy server.<br>The server should have a network interface with the assigned IP address. |
| TM Enterprise server | Less than 10 GB/day | SATA, 600 GB | 2CPU 8xC + Hyper-threading<br>(Intel® Xeon® Processor E5-2640 v3 2,6 Hz) | 32 GB | | |
| | From 10 GB/day to 50 GB/day | SATA/SAS, RAID5, 6+ HDD | 2SRVx2CPU 10xC | 64 GB | | |
| | More than 50 GB/day | SAS, rack | Calculated on demand | 64 GB for each server | | |
| Database | Oracle | 3,6 TB | 2CPU 6xC, | 32 GB | | Provides storage for |

| | | | | | | |
|---|---|---|---|---|---|---|
| server | PostgreSQL | | 2,6 Ghz | 24 GB | | traffic of 1-2 ths. users by 3 months; without OCR, without Device Monitor |

| | | | | | |
|---|---|---|---|---|---|
| Crawler Server and Crawler Scanner | 1 GB of free space - for the server; at least 10 GB of free space - for the scanner: required for temporary storing of files copied from examinee resources | 2 cores or higher | 2 GB | • OS:<br>  ○ Microsoft Windows Vista 7 / 8 SP2<br>  ○ Microsoft Windows Server 2008 R2 SP1 or SP2 / 2012<br>  ○ Microsoft Windows 7 SP1<br>• Microsoft .Net Framework 4.5 | • **iw_expressd** process autoun should be enabled on the TM server (see details in «*InfoWatch Traffic Monitor. Administration Guide*» )<br>• Both Crawler Server and Scanner should be installed on computers located in the same domain which includes all workstations supposed to be scanned.<br>• It is recommended that a computer where Crawler scanner works should be located in the network segment maximum close to segments to be scanned. Otherwise, the network load may increase significantly.<br>• If network segments where InfoWatch Traffic Monitor with Crawler is deployed are divided by firewalls, then for correct operation of Crawler, the **1337** TCP port (Traffic Monitor connects to Crawler server) and **6556** TCP port (Crawler scanner connects to Crawler server) must be opened. |

You also can install the System to the virtual environment: VMware, MS Hyper-V or other virtualization system.

# 3 INSTALLING THE SYSTEM

**Note:**

After the System installation, a trial license will be automatically loaded into the System (for more information on licensing, see the document «*InfoWatch Traffic Monitor. Administration Guide*»).

This section contains instructions on each type of the System installation.

See information on how to choose the installation type in "System Deployment Schemes and Installation Types".

Details on deployment this schemes in the existing infrastructure are described in «*InfoWatch Traffic Monitor. Administration Guide*».

**Warning!**

Before installation, make sure that environment where the System will be deployed meets software and hardware requirements (see "Hardware and Software Requirements").

Installation of the server components of the InfoWatch Traffic Monitor system is performed using installer program (**kickstart**).

The set of installed components differs depending on the server purpose:

| Server purpose | Kickstart key | Components installed by kickstart |
|---|---|---|
| All InfoWatch Traffic Monitor (Enterprise or Standard) components on the same computer | **TME All-in-one**<br>**TMS All-in-one** | • Installing OS Linux<br>• Configuring network interface<br>• Installing and configuring DBMS Oracle or PostgreSQL<br>• Installing IW Traffic Monitor database schema<br>• Installing RPM packages of IWTM Server<br>• Installing Monitoring subsystem<br>• Installing Management console |

| | | |
|---|---|---|
| DBMS Server with Traffic Monitor DB schema on a separate computer | **TME DB server** | • Installing OS Linux<br>• Configuring network interface<br>• Installing and configuring DBMS Oracle or PostgreSQL<br>• Installing IW Traffic Monitor database schema |
| Traffic Monitor Server on the separate computer | **TME Node server** | • Installing OS Linux<br>• Configuring network interface<br>• Installing RPM packages of IWTM Server<br>• Installing Monitoring subsystem<br>• Installing Management console |
| All InfoWatch Traffic Monitor (Enterprise or Standard) components<br>on the same computer in the simplified mode | **TME Appliance**<br>**TMS Appliance** | • Installing OS Linux<br>• Configuring network interface<br>• Installing and configuring DBMS Oracle or PostgreSQL<br>• Installing IW Traffic Monitor database schema<br>• Installing RPM packages of IWTM Server<br>• Installing Monitoring subsystem<br>• Installing Management console |

You can find information on the desired installation type in the following articles:

- General Information on Installation Steps
- All-in-one Installation Mode of TM Enterprise and TM Standard
- Distributed Installation of TM Enterprise
- Installation of TM Appliance Standard and TM Appliance Enterprise
- Installing the Crawler Subsystem (optional)

Information on pre-installed accounts see in "Pre-installed Server Settings".

When installation of the server components is finished, the Management console is available through the browser window by entering the URL:

- of the Traffic Monitor Server – if All-in-one installation mode is used or TM Appliance installed;
- of the primary Traffic Monitor Server – if the System components are installed on different computers.

Information on allocating of the primary server in a distributed installation mode is provided in *InfoWatch Traffic Monitor. Administration Guide*», "Additional Settings when Installing with TME DB Server and TME Node Server keys" article.

# 3.1 General Information on Installation Steps

This section contains a description of steps which are common for all installation types:

- Start Window
- Selecting the Database
- Selecting the Installation Mode
- Choosing a Time Zone
- Setting Password for System Superuser
- Choosing a Disk Partitioning Method
- Network Settings
- Configuring Time Synchronization (NTP-server)
- Localization Settins
- Configuring the Automatic Event Deletion from the Database
- Completing the Installation

## 3.1.1 Start Window




The first screen of the Installation Wizard (**kickstart**) allows you to select one of the following actions:

- **TM Enterprise** – begins InfoWatch Traffic Monitor Enterprise installation
- **TM Standard** – begins InfoWatch Traffic Monitor Standard installation
- **Boot from local drive** – loads from a local computer disk

- **Rescue installed system** – emergency recovery of InfoWatch Traffic Monitor system. This option should be used by InfoWatch engineers only
- **Memory test** – hardware test (can take some time). Can be used as an auxiliary option if necessary

**Note:**

To review additional loading options press **F1**.
Due to their complexity, additional options should be used by InfoWatch engineers only.

## 3.1.2 Selecting the Database




When you have the System edition (Enterprise or Standard) selected, you will be prompted to select the DBMS for the System:

- **DB - Oracle** (**Standard** or **Enterprise**, depending on edition selected on the previous step)
- **DB - PostgreSQL**.

Details on installation type selecting see in "System Deployment Schemes and Installation Types".

Press **Enter**.

### 3.1.3 Selecting the Installation Mode

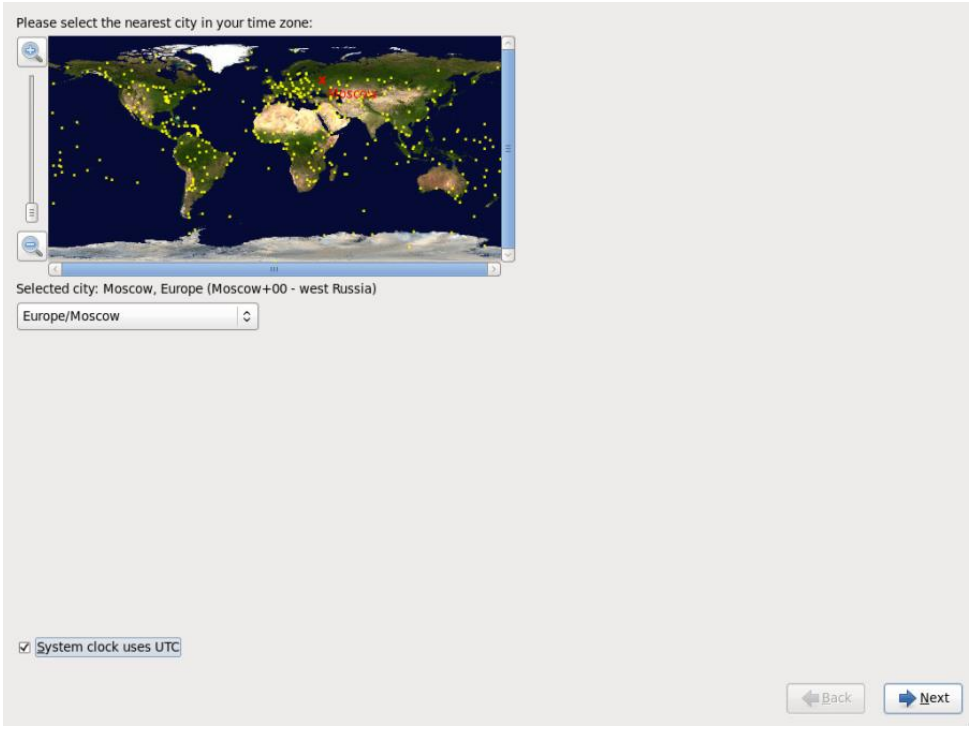



When you have selected the DBMS, you will be prompted to select the installation mode. The set of modes depends on what you selected at the previous steps. The can be the following modes:

- **TME/TMS Appliance** (**PostgreSQL** or **Oracle**) – System installation in Appliance mode which provides the simplified integration. See details on this type of installation in "Installation of TM Appliance Standard and TM Appliance Enterprise".
- **TME/TMS All-in-one: TM+DB server** (**PostgreSQL** or **Oracle**) – all System components (with Oracle DBMS or PostgreSQL) are installed on the same server. This installation type is used if, with respect to the assumed load, the server has resources for DBMS and TM services. See details in "All-in-one Installation Mode of TM Enterprise and TM Standard".
- **TME/TMS DB server** (**PostgreSQL** or **Oracle**) – installation of the database together with a selected DBMS on the separate computer. See details in "Installing Database (TM DB Server)".
- **TME/TMS Node server** (**PostgreSQL** or **Oracle**) – installation of the Traffic Monitor Server on a separate computer. See details in "Installing Traffic Monitor Server (TME Node Server)".

See details on chosing the installation mode in "System Deployment Schemes and Installation Types".

### 3.1.4 Choosing a Time Zone




Specify settings of the time zone for the server.

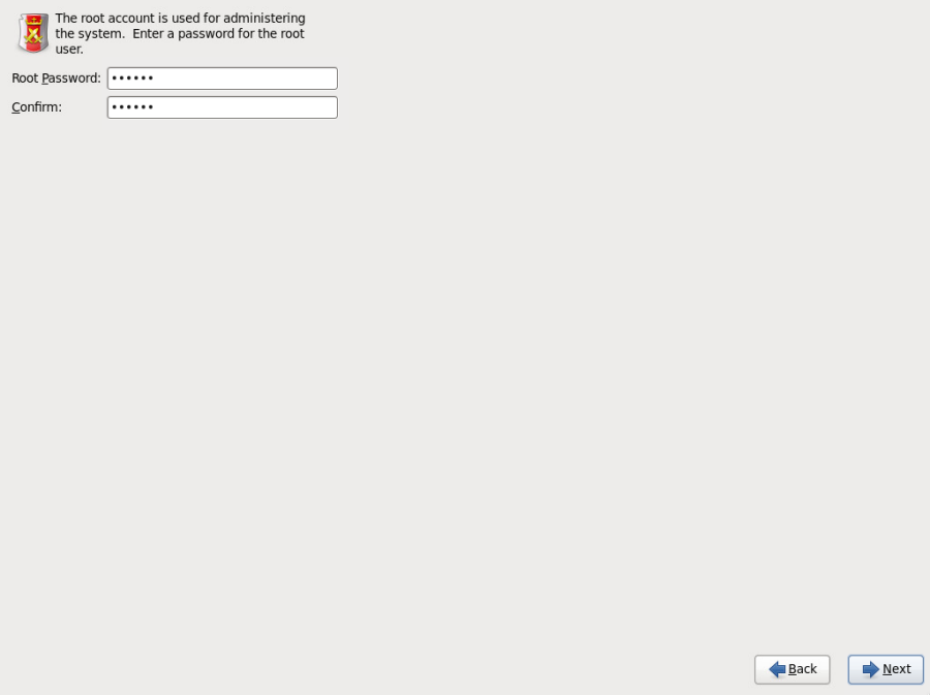
You can find your city:

- In the drop-down list. The cities are sorted based on a part of the world they belong to. For example, Moscow is included into Europe group;
- On the map. For navigation, use a scroll-bar and scale buttons.

Mark the **System clock uses UTC** checkbox if system time is set to Greenwich time (UTC).

Click **Next**.

## 3.1.5 Setting Password for System Superuser




*root* user is the System superuser. For the *root* user, a password must be specified.
In case your password does not match safety requirements, you will see a warning **Weak Password**. Use the following buttons:

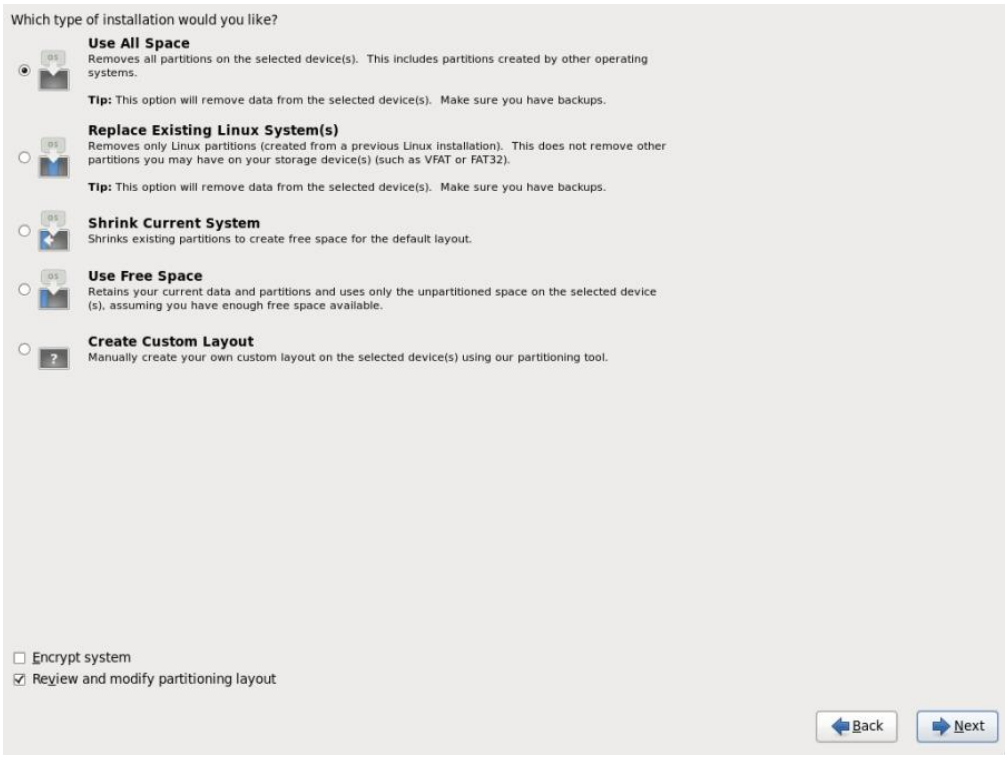
- **Use anyway** – if you want to use an entered password despite recommendations;
- **Cancel** – if you want to change the entered password.

> **Note:**
> Recommendations on password creation are available in Appendix A .

## 3.1.6 Choosing a Disk Partitioning Method

> **Warning!**
> When the System is installed, its components are located in the following directories:
- InfoWatch Traffic Monitor – `/opt/iw`;
- Database – `/u01` and `/u02` (for TM version `6.1.100` and earlier, DB PostgreSQL is installed only

to `/u01`).
If TM Server and DB are installed separately (see "Distributed Installation of TM Enterprise" then those directories will be located on different servers.

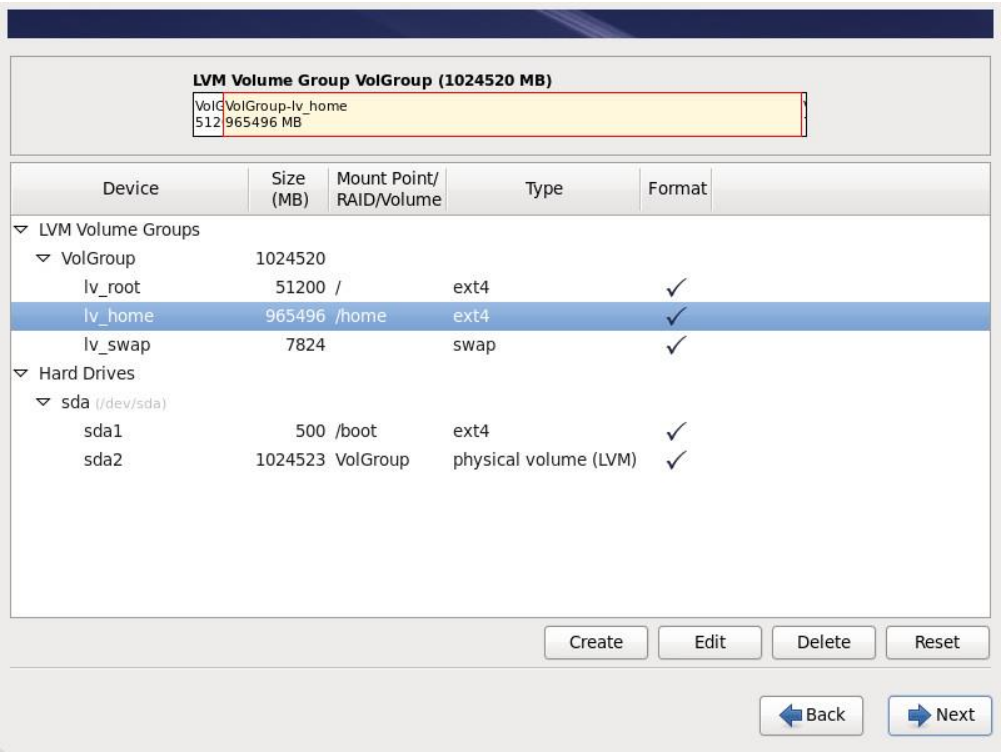



We recommend re-splitting the disc space in the following ratio:

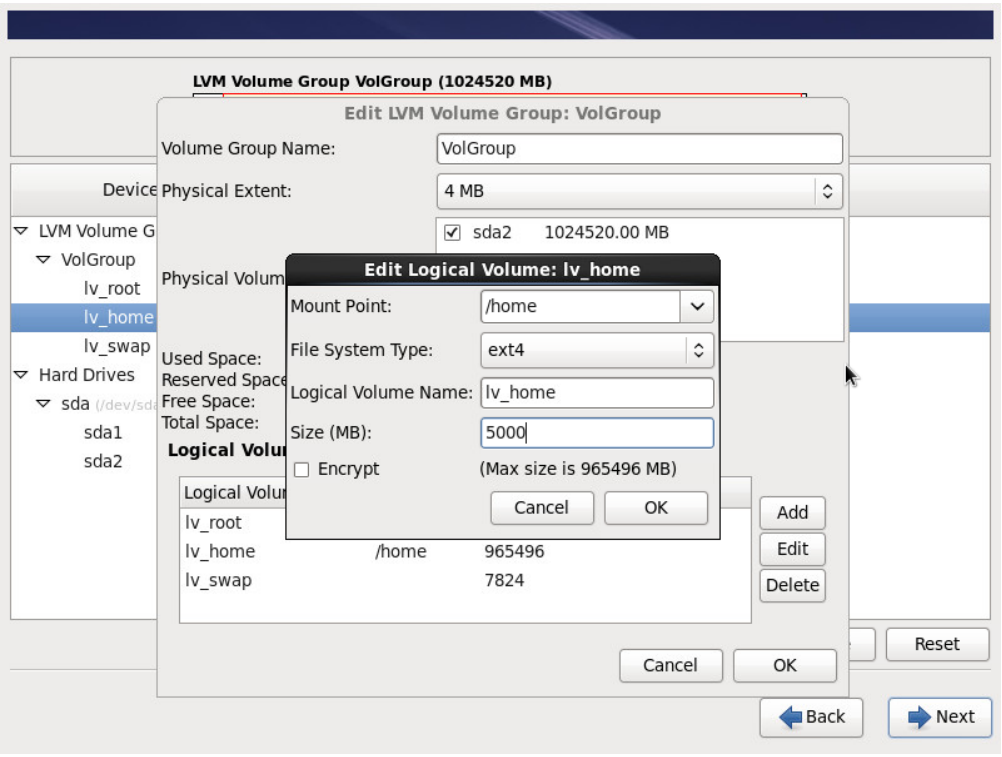
- **home** partition - 5 GB;
- **SWAP** partition - default value;
- **root** partition - all remain space.

To perform this partitioning:

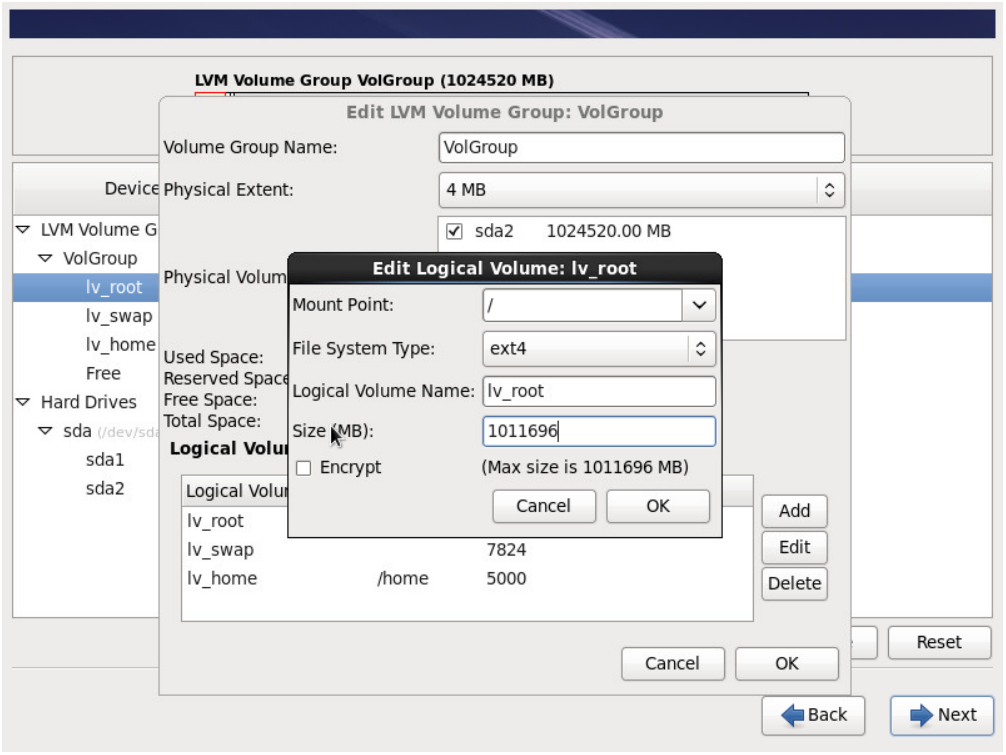
1. Select **Use All Space** – all partitions of the selected device(s) will be deleted, including partitions created by other operating systems. *All information will be deleted, so remember to backup all necessary data.*
2. Check the **Review and modify partitioning layout** box in the bottom of the window - this lets you to view and modify disk partitions.
3. Click **Next**.
4. In **Please Select A Device** select **lv_home** partition and click **Edit**.




5. In **Size (MB)** field specify**5000**. Click **OK**.




6. In **Please Select A Device** window select **lv_root** partition and click **Edit**.
7. In **Size (MB)** field specify all remain free space (displayed under the field - **Max size is...**). Click **OK**.

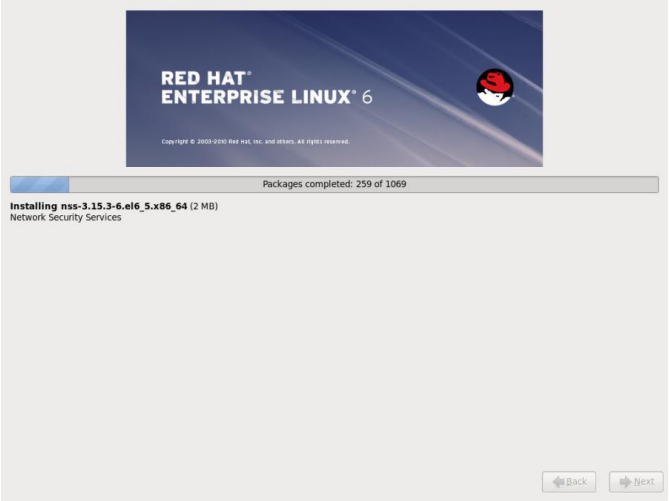



8. In **Please Select A Device** window click **Next**.

The process of disk partitioning and OS installation will be started.

> **Note:**
>
> The **Format Warnings** window can be displayed reminding that hard disk volumes used for installation will be formatted. Click **Format** to continue installation.

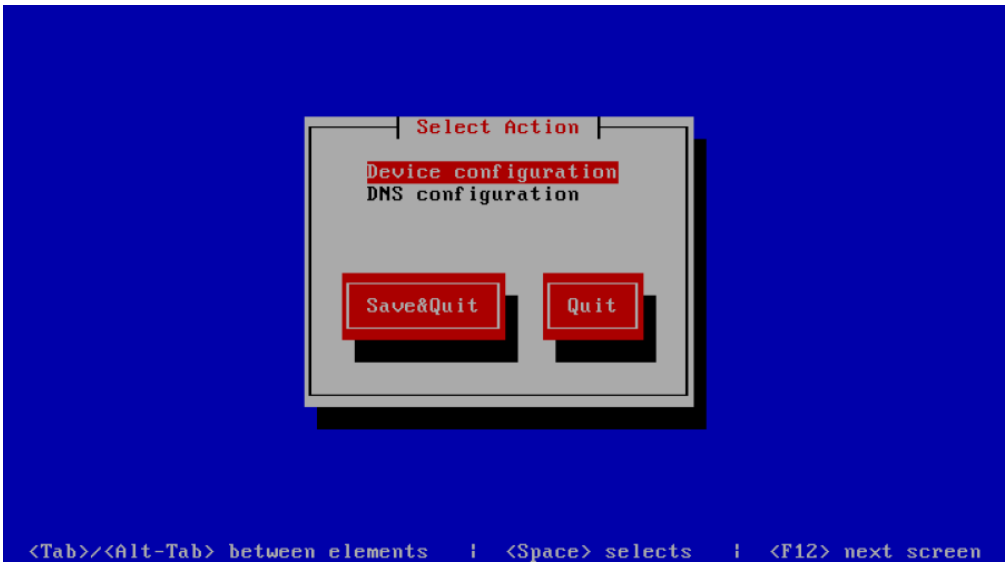
The progress will be displayed on the screen:



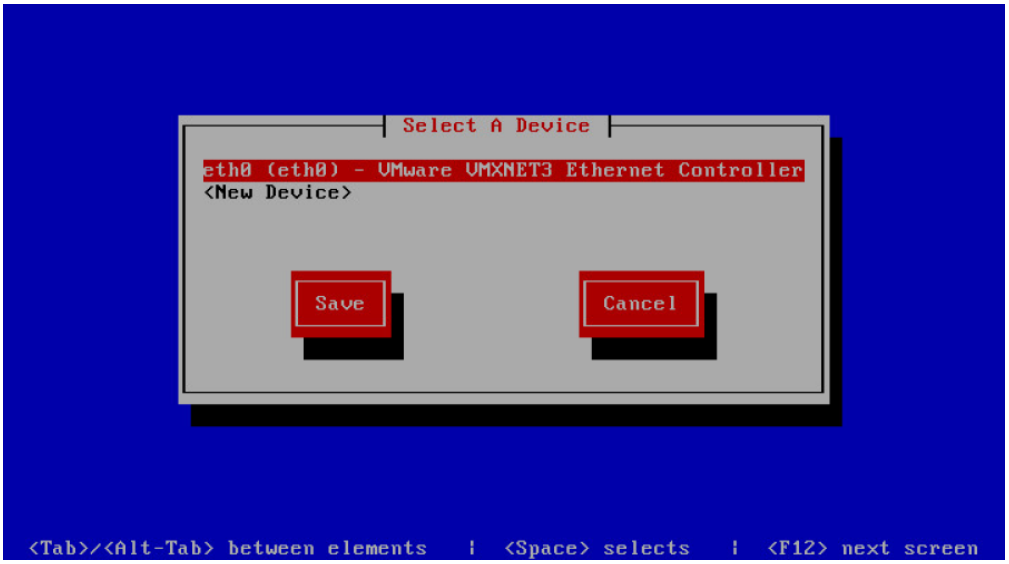
The process can take some time.

When the operating system will be installed, the computer reboots and network settings will be prompted to configure (see "Network Settings").

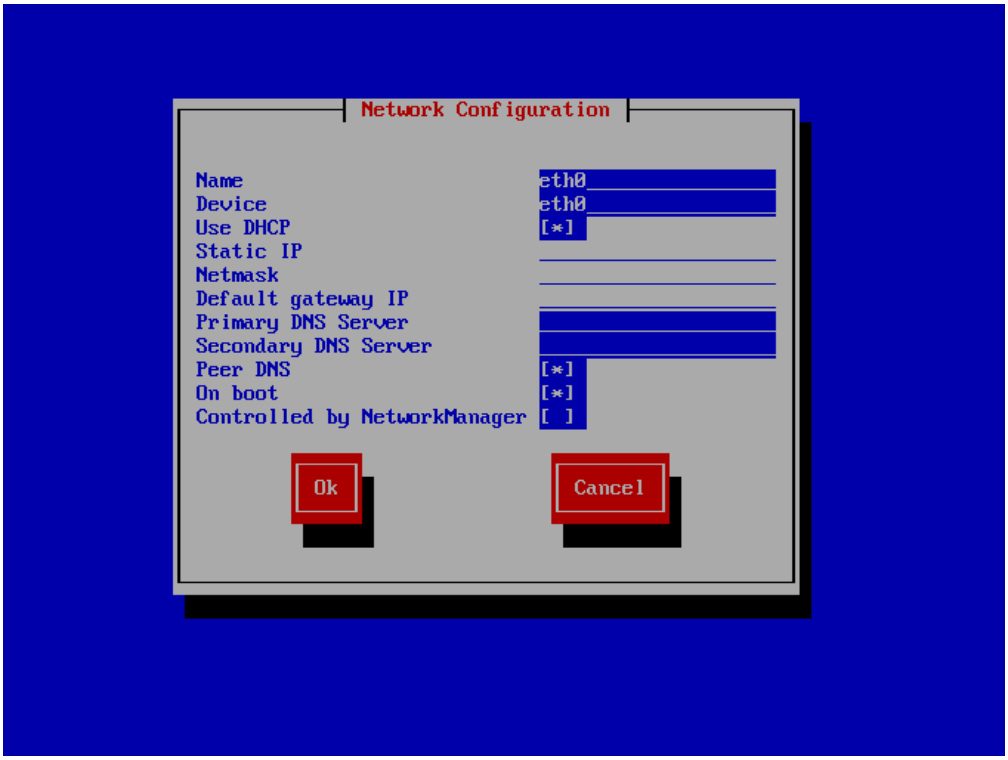
## 3.1.7 Network Settings




1. To set up parameters of a network card:
    a. In the **Select Action** window select **Device configuration** and press **Enter**.




    b. In the **Select A Device**window select network interface **eth0** and press **Enter**.
    c. if you want the System to use network settings from DHCP server, set the cursor in the **Use DHCP** field and click space. Otherwise enter network settings manually (static IP address and so on). Upon completing click **Ok**.

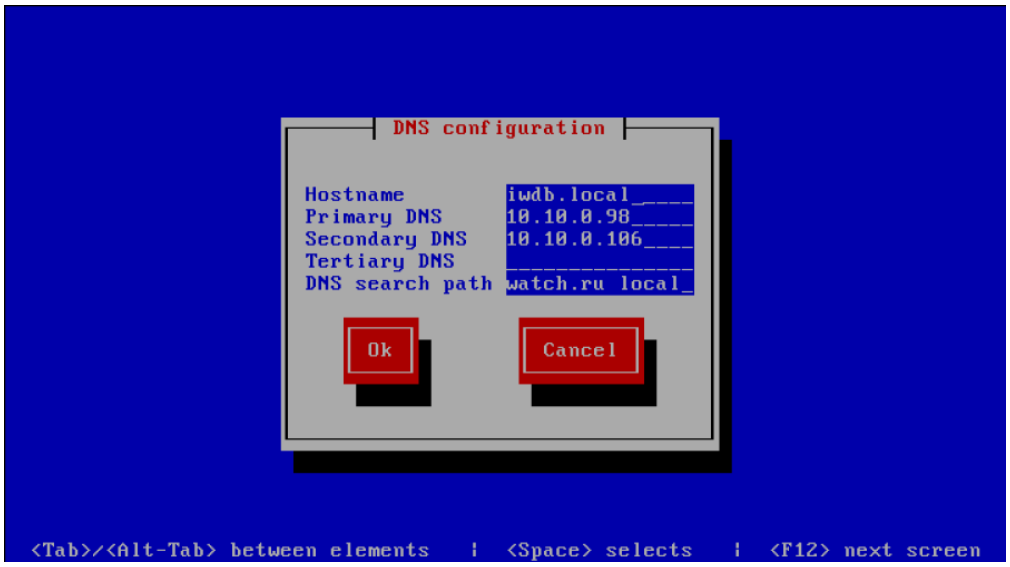



> **Warning!**
>
> Do not use **Controlled by NetworkManager** option.

> **Warning!**
>
> When using **Use DHCP** setting, the System will use only data gained from specified DHCP servers. Data entered to the **DNS configuration** window (see further) will be ignored. If you change `/etc/resolv.conf` file manually, iths data will be replaced by gained from DHCP server after the next server reboot.

d. Click **Save** to save settings.

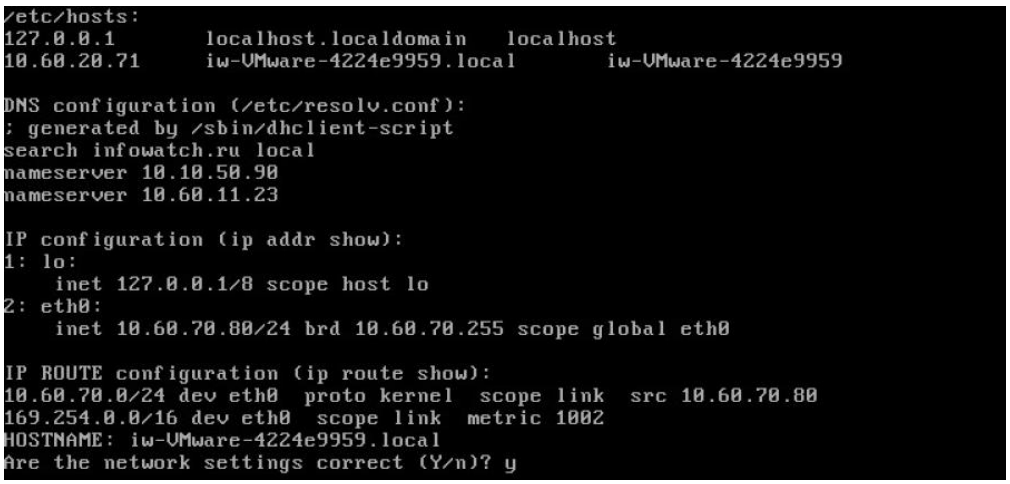
2. To configure DNS configuration in the **Select Action** window select **DNS configuration** and specify needed network settings of the server. Then click **Ok**.




**Warning!**

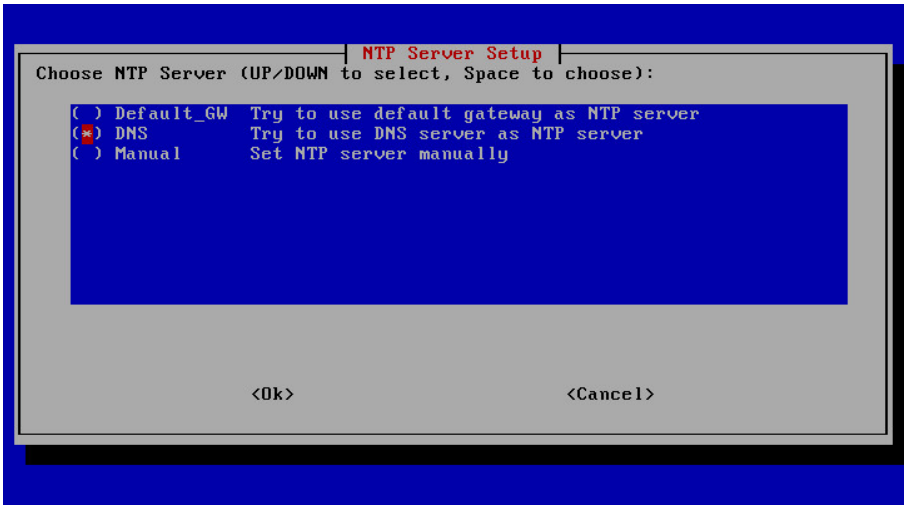
If you select **Use DHCP** in the **Network Configuration** window then instaed of parameters you specified the ones received fron DHCP will be used.

3. Click **Save&Quit**.



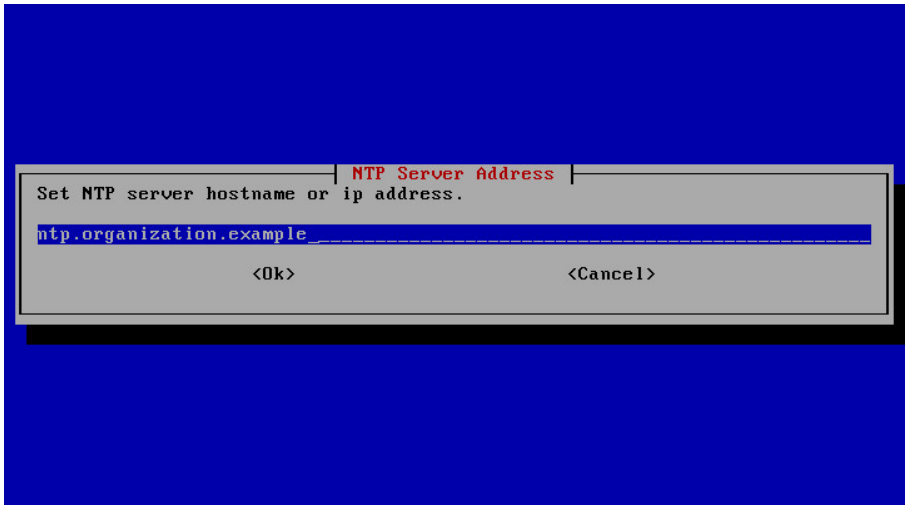

4. Examine the network settings you specified. If settings are wrong, enter **N** and specify the correct ones (see previous steps) If settings are correct, enter **Y** to confirm and press **Enter**.

## 3.1.8 Configuring Time Synchronization (NTP-server)



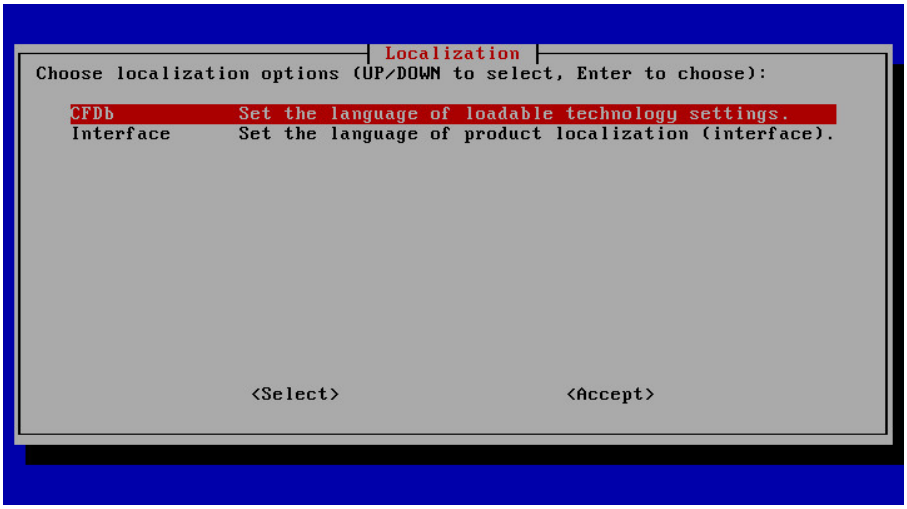

You can select one of three server setup options for time synchronization (NTP-server). Set asterisk symbol ( * ) in the required field and press space then click **OK**.

- **Default_GW** - default gateway
- **DNS** - domain controller: usually used in organizations as a time server
- **Manual** - you cen manually specify server name of IP address.



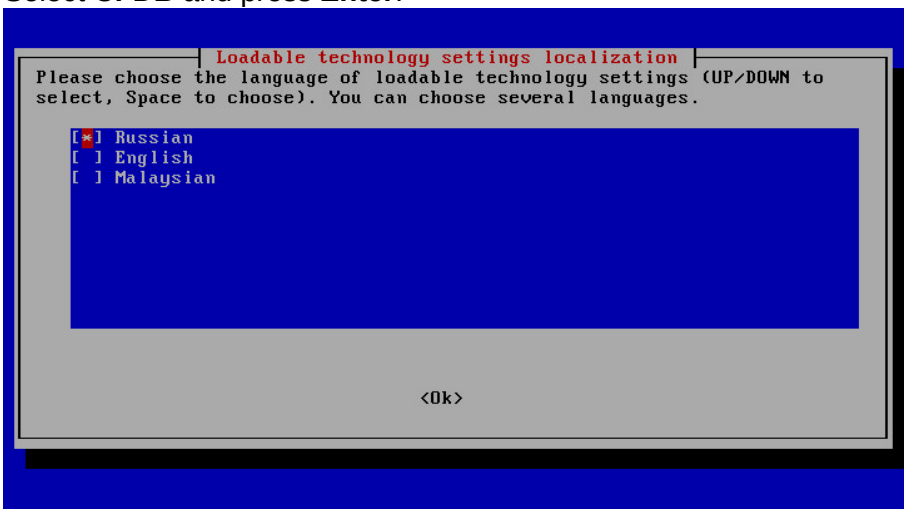

If NTP server cannot be specified for some reasons, click **Cancel** and set this parameter later; details on configuring the NTP server see in «*InfoWatch Traffic Monitor. Administration Guide*».

## 3.1.9 Localization Setting




To specify System localization parameters:

1. Specify language settings for such preinstalled units as categories and terms, списки, preinstalled filters and default policies:
   a. Select **CFDB** and press **Enter**.



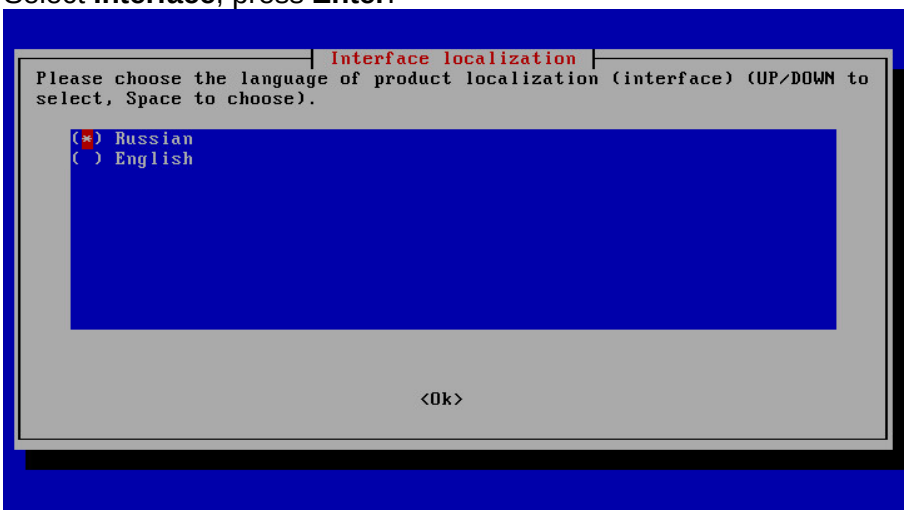

   There are three languages available::

   - *Russian* – to install the Classifier in Russian;
   - *English* – to install the Classifier in English;
   - *Malaysian* – to install the classifier in Malaysian.

   To select the language set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared. You can select one, two or three languages.

   b. Press **OK**.
2. Specify language for Management Console:

a. Select **Interface**, press **Enter**.

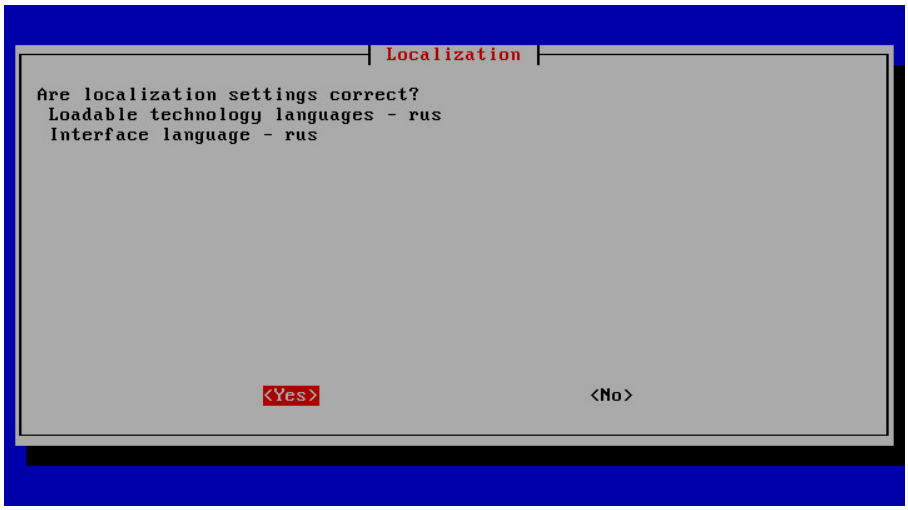



There are two languages available:

- *Russian* – to install interface in Russian;
- *English* – to install interface in English.

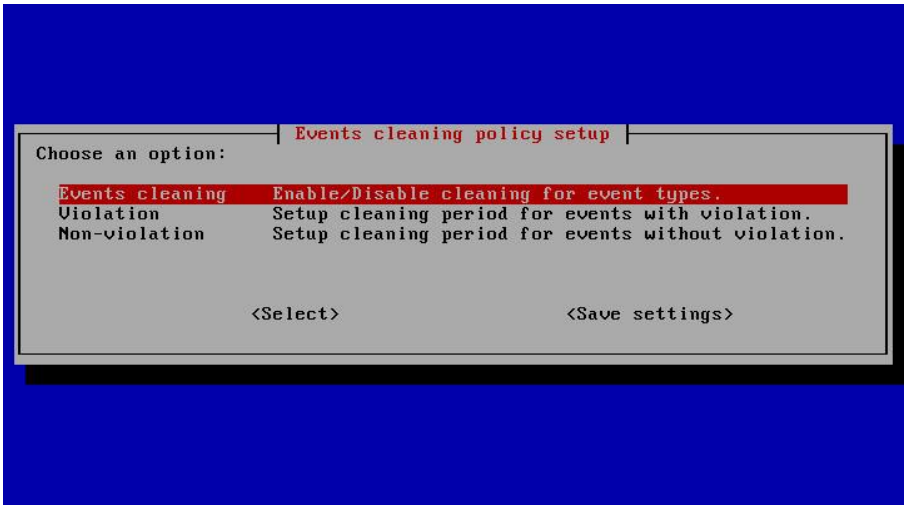
b. select required interface language and press **OK**.

3. After selecting localization parameters, press **Accept**.



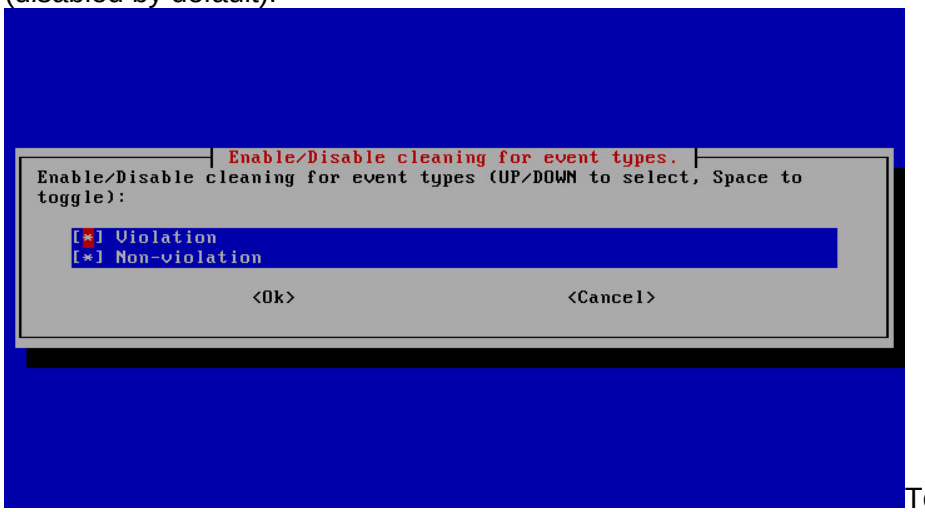

4. In the opened window check, whether parameters have been specified correctly, press **Yes**.

## 3.1.10 Configuring the Automatic Event Deletion from the Database



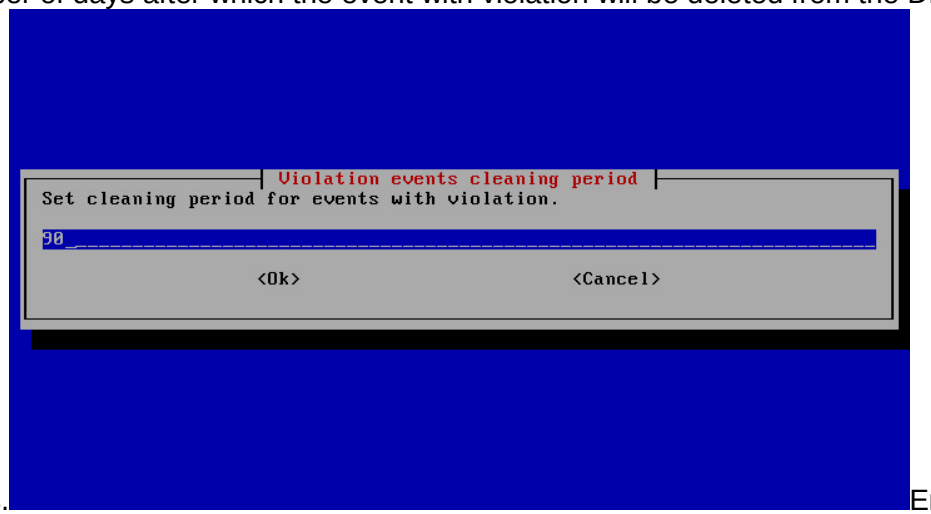

Configure settings of automatic deletetion of events from the DB. To do this select one of three options then click **Select**:

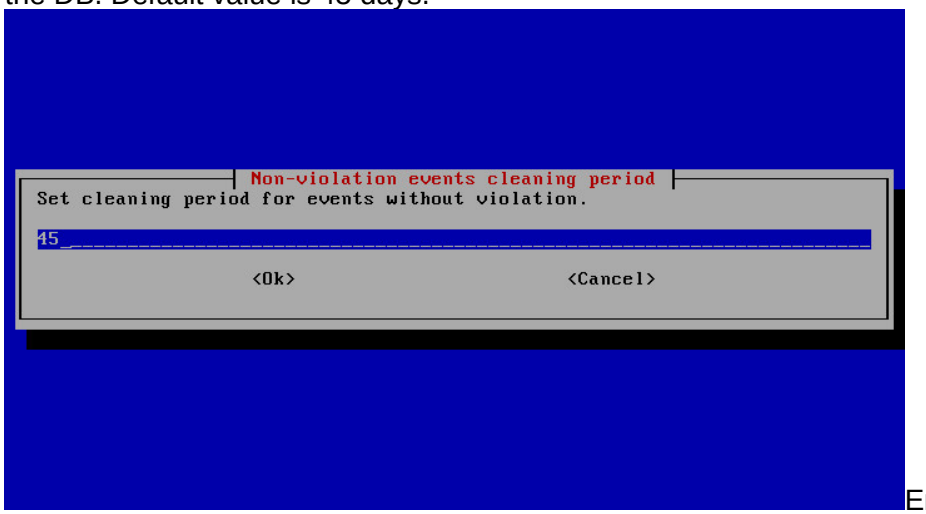
- **Events cleaning** – configures enabling and disabling of the automatic deletetion of two event types (disabled by default).




To select the option set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared:

  - **Violation** – enables automatic deletetion of events which violate the security policy (see details on policies in "*InfoWatch Traffic Monitor. User Guide*")
  - **Non-violation** – enables automatic deletetion of events which do not violate the security policy of the company.
    You can select both items to delete both violating and not violating events.
    Click **Ok**.

- **Violation** – sets a number of days after which the event with violation will be deleted from the DB. Default value is 90 days. 

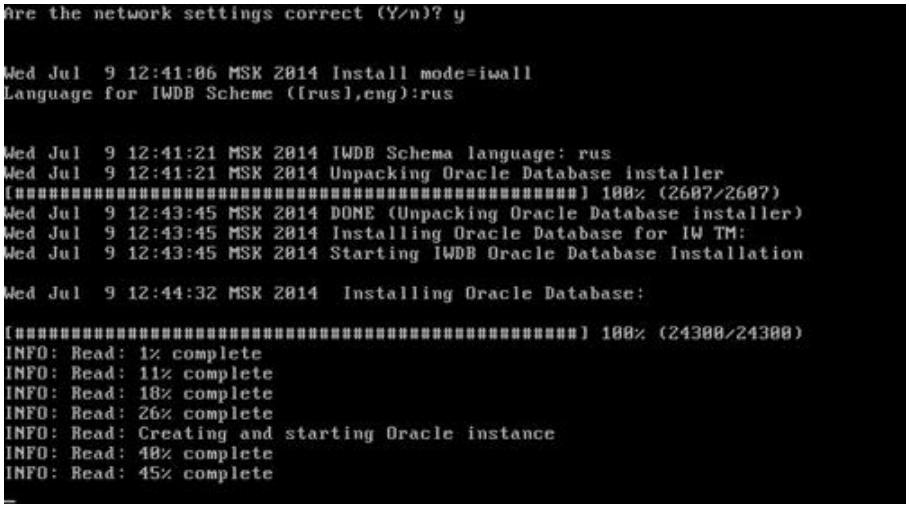
Enter the period of deletion, in days. Click **Ok**.
- **Non-violation** – sets a number of days after which the event without violations will be deleted from the DB. Default value is 45 days.


Enter the period of deletion, in days. Click **Ok**.

When all settings are finished, click **Save settings**.

## 3.1.11 Completing the Installation

Upon the settings are configured, the DBMS and DB schema begins. The progress will be displayed on the screen:




During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where xxxxxxxxxxxxxxx is the Serial Number of a server.

See details on further System configuration in «*InfoWatch Traffic Monitor. Administration Guide*».

## 3.2 All-in-one Installation Mode of TM Enterprise and TM Standard

All-in-one installation mode allows installing all components of the System on the same computer.

> **Warning!**
>
> This chapter contains instructions without a detailed description of installation screens. For additional information, see «General Information on Installation Steps».

**To install the Traffic Monitor Enterprise or Traffic Monitor Standard in All-in-one mode, perform the following steps:**

1. Connect the distribution disk: the installation program (kickstart) will run automatically.
2. In the Welcome window, select:
   - **TM Enterprise** – to install Enterprise edition
   - **TM Standard** – to install Standard edition.

   Then press **Enter**.
3. In the window of the Database selection, please select the required DBMS:
   - **Oracle** (Standard or Enterprise depending on edition selected at the previous step)

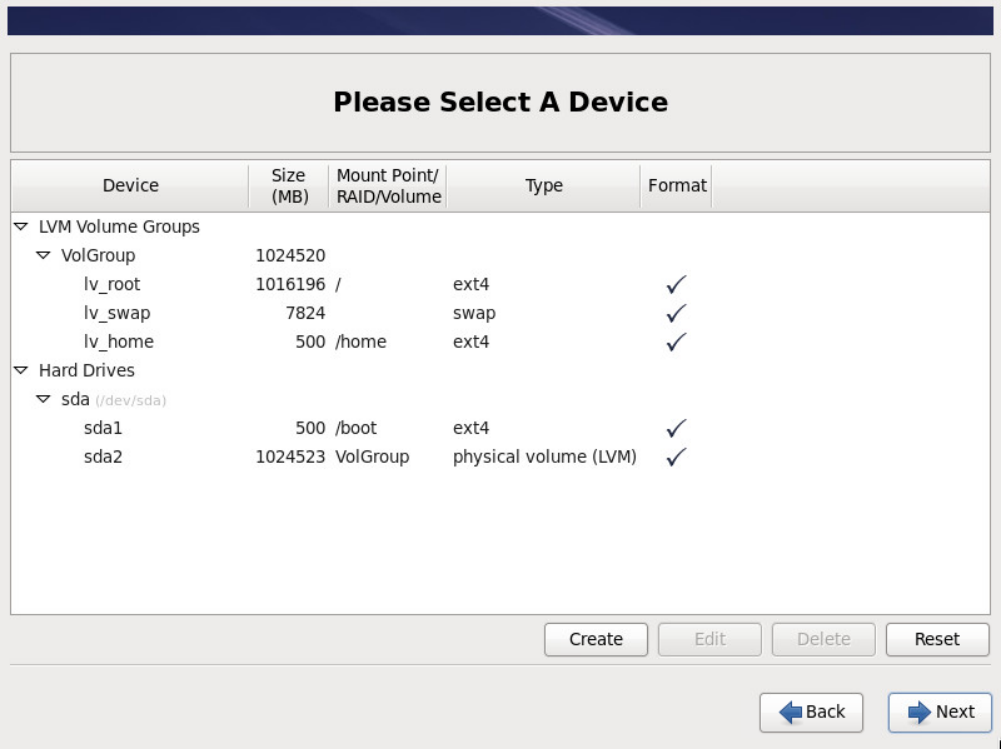
- **PostgreSQL**

Then press **Enter**.

4. In the window of installation mode selection, choose **TME All-in-one** or **TMS All-in-one** and press **Enter**.

> **Warning!**
>
> When the installation mode is selected, the following warning message may appear: «*The storage device below may contain data*». To clean the disk and start the installation, click **Yes, discard any data** and leave the field **Apply my choice to all devices with undetected partitions of file systems** unchanged.

5. Specify time zone settings for the server (if the system time is set by Greenwich (UTC), select the field **System clock uses UTC**) and click **Next**.
6. Specify a password for *root* superuser and click **Next**. Recommendations on password creation are available in Appendix A .
7. Specify the mode of disk space partitioning (see detailed description in "Choosing a Disk Partitioning Method"):
   a. Select **Use All Space**.
   b. Select the checkbox **Review and modify partitioning layout**.
   c. Click **Next**.
   d. In **Please Select A Device** select **lv_home** partition and click **Edit**.
   e. In **Size (MB)** field specify**5000**. Click **OK**.
   f. In **Please Select A Device** window select **lv_root** partition and click **Edit**.
   g. In **Size (MB)** field specify all remain free space (displayed under the field - **Max size is...**). Click **OK**.

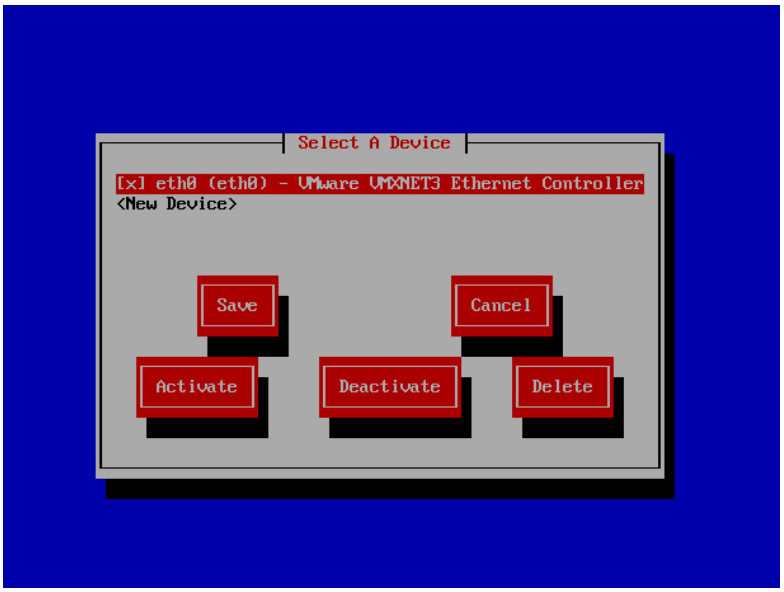



h. Click **Next**.

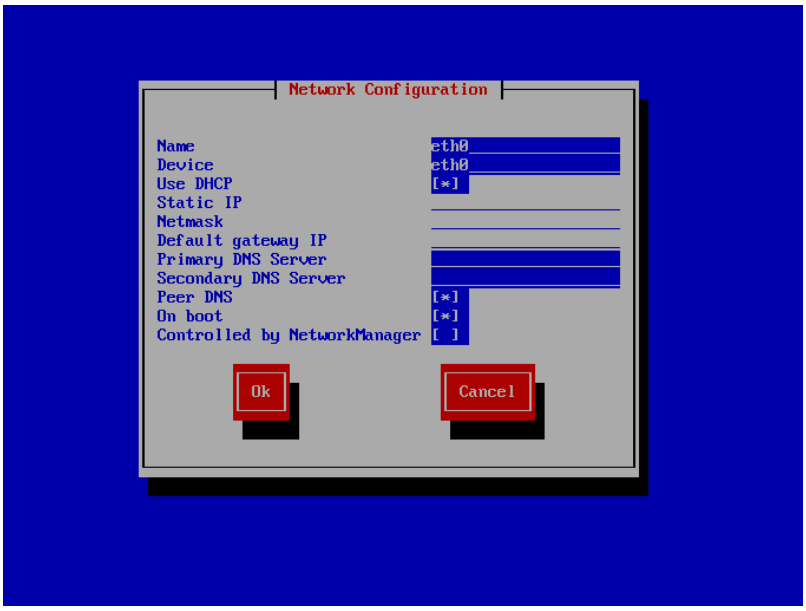
> **Note:**
>
> The **Format > Warnings** window can be displayed which informs you that hard disk partitions, which will be used for installation, need formatting. To continue the installation, click **Format** .

The disk partitioning and operating system installation will start. Progress will be displayed on the screen.
The process may take some time.
When installation of the operating system is completed, the system will be restarted and you will be prompted to configure network parameters:

8. To configure parameters of a network card:
   a. Select **Device configuration** and press **Enter**.




b. Select network interface **eth0** and press **Enter**.




> **Warning!**
>
> Please do not enable **Controlled by NetworkManager** option.

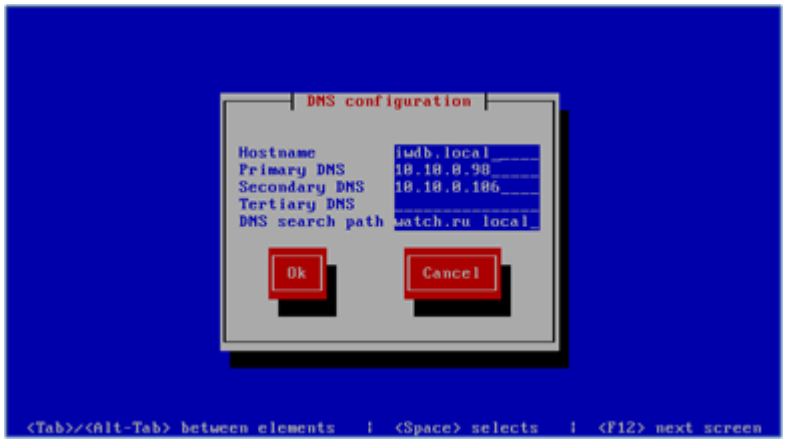
c. If you want network settings of DHCP server to be used in the System, move the cursor to the **Use DHCP** field and press Space. Otherwise, specify network settings for the server manually (static IP-address of the computer, etc.). Upon completion, click **OK**.

**Warning!**

With **Use DHCP** setting enabled, the system will use only data received from specified DHCP servers. Data from the **DNS configuration** dialog (see below) will be ignored. If you change the `/etc/resolv.conf`file manually, its data will be replaced with the data received from DHCP server at the next restart of the system.

d. Click **Save** to save settings.

9. To configure DNS, select **DNS configuration** and specify required server's network parameters. Then click **OK**.




**Warning!**

If in the **Network Configuration** dialog the **Use DHCP** option was selected, these parameters will be replaced with those received from specified DHCP servers .

10. Click **Save&Quit**.
11. Check specified network settings. If they are incorrect, type **N** and specify correct parameters (see previous steps). If the settings are correct, type **Y** to confirm and press **Enter**.
12. Specify the server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field and press Space, then click **OK**.

**Note:**

If NTP server cannot be specified for some reasons, click **Cancel** and set this parameter later (details on configuring the NTP server see in "*InfoWatch Traffic Monitor. Administration Guide*»).

13. Set localization settings:
    a. Set the language of pre-installed settings:
        i. Select **CFDB** and press **Enter**.

ii. Specify the desired language and click **OK**.

The selected language will be used when creating terms and categories, filters and default policies.

b. Set interface language:

i. Select **Interface**and press **Enter**.

ii. Specify the desired language and click **OK**.

The Management console will be installed in selected language.

c. Click **Accept**.

d. In the opened window make sure the selected languages for pre-installed settings and interface are specified correctly, then click **Yes**.

14. Set parameters of automatic events deletion from DB.
Select one from three options then click **Select**:

- **Events cleaning** – sets enabling and disabling the automatic deletion of two event types (disabled by default ).
To select the option set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared:
  - **Violation** – enables automatic deletion of events which violate the security policy (see details on policies in "InfoWatch Traffic Monitor. User Guide")
  - **Non-violation** – enables automatic deletion of events which do not violate the security policy of the company.
  You can select both items to delete both violating and not violating events.

  Click **Ok**.
- **Violation** – sets a number of days after which the event with violations will be deleted from the DB (default: 90 days).
Enter the period of deletion, in days. Click **Ok**.
- **Non-violation** – sets a number of days after which the event without violations will be deleted from the DB (default: 45 days).
Enter the period of deletion, in days. Click **Ok**.

  When all settings are finished, click **Save settings**.

The installation of the DBMS and a DB scheme will start. The progress of both processes will be displayed on a screen.

The process may take some time.

During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where xxxxxxxxxxxxxxx is the Serial Number of a server.

Web Console installation is performed in an automatic mode. After the completion of the server-end installation the Management console is available through a browser: enter the URL of the Traffic Monitor Server.

The procedure of further System configuration is described in the document «*InfoWatch Traffic Monitor. Administration Guide*»

## 3.3 Distributed Installation of TM Enterprise

The Enterprise edition of the Traffic Monitor system allows you to deploy the System so that Traffic Monitor Server and DBMS (Oracle Enterprise or PostgreSQL) are installed on the different computers. Such installation is used if Traffic Monitor Server services and DBMS cannot efficiently operate on the same computer with respect of the supposed load.

Server installation is performed in the following order:

- Installing Database (TM DB Server)
- Installing Traffic Monitor Server (TME Node Server).

> **Warning!**
>
> Installation in a different order (Traffic Monitor Server is installed before the Database) is not supported and results in error messages during the installation.

You can install several Traffic Monitor Servers. At that you shold logically divide them into primary one and secondary one(s). The primary server is one where all processes needed for the System in a single copy are running. Details on servers configuring see in "*InfoWatch Traffic Monitor. Administrator Guide*", "*Additional Settings when Installing with TME DB Server and TME Node Server Keys*" article.

### 3.3.1 Installing Database (TM DB Server)

the

> **Warning!**
>
> This chapter contains instructions without a detailed description of installation screens. For additional information, see "General Information on Installation Steps".

**To install a database, perform the following steps:**

1. Connect the distributive disk: the installation program (kickstart) will run automatically.
2. In the Welcome window select **TM Enterprise** and press **Enter**.
3. In the database selection window specify which DBMS should be installed:
    a. Oracle Standard;

b. PostgreSQL.

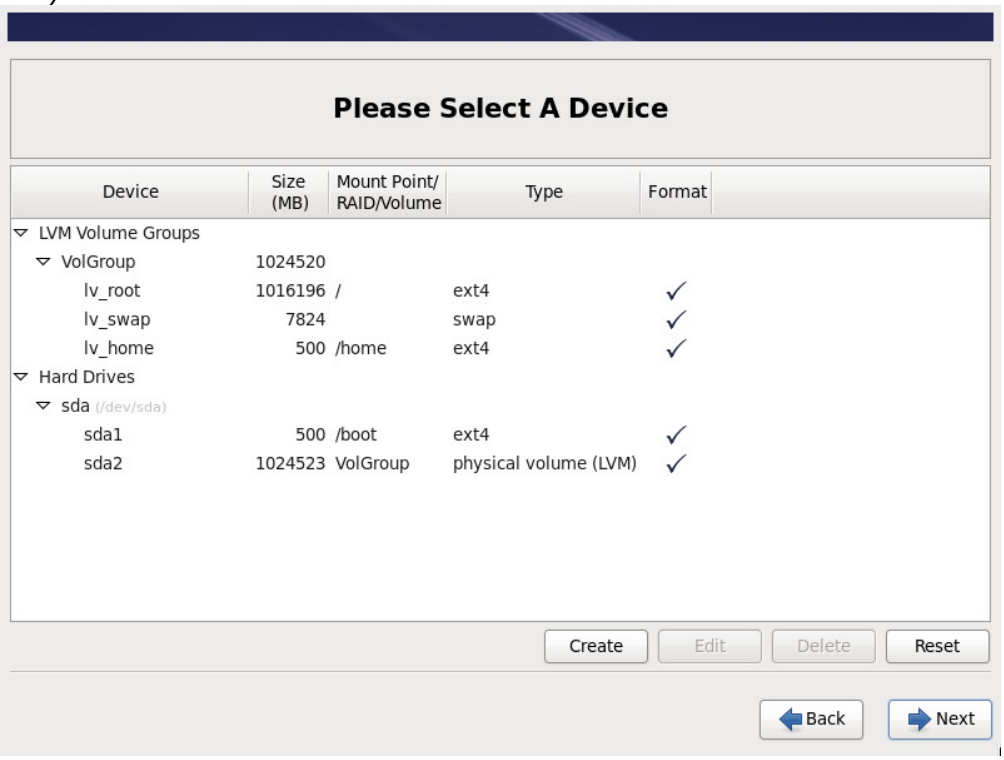
Click **Enter**.

4. In the window of selecting the installation mode, choose **TME DB server** and press **Enter**.

> **Warning!**
>
> When the installation mode is selected, the following warning message may appear: "*The storage device below may contain any data"*. To clean a disk and start the installation, click **Yes, discard any data** and left the **Apply my choice to all devices with undetected partitions of file systems** field unchanged.

5. Specify time zone settings for a server (if the system time is set by Greenwich (UTC), place a check mark to a field **System clock uses UTC**) and click **Next**.
6. Specify a password for *root* superuser and click **Next**. Recommendations on password creation are available in Appendix A
7. Specify the mode of disk space partitioning (detailed description see in "Choosing a Disk Partitioning Method"):
   a. Select **Use All Space**
   b. Select the checkbox **Review and modify partitioning layout**
   c. Click **Next**
   d. In the **Please Select A Device** window, select **lv_home** partition and click **Edit**.
   e. In the **Size (MB)** field, specify **5000**. Click **OK**.
   f. In the **Please Select A Device** window, select **lv_root** partition and click **Edit**.

g. In the **Size (MB)** field, specify **all remain free space** (displayed under the field - **Max size is...**). Click **OK**.




h. Click **Next**.

The disk partitioning and installation of the operating system will start. Progress will be displayed on a screen.
The process may take some time.

When installation of the operating system is completed, the system will be restarted and you will be prompted to configure network parameters.

8. Configure parameters of a network card and DNS as described in "Network Settings". Click **Save&Quit**.
9. Check specified network settings. If they are incorrect, type **N** and specify correct parameters (see previous steps). If the settings are correct, type **Y** to confirm and press **Enter**.
10. Specify server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field and press **Space**, then click **OK**.
11. Set localization settings:
    a. Set the language of pre-installed settings:
        i. Select **CFDB** and press **Enter**.
        ii. Specify the desired language and click **OK**.

    The selected language will be used when creating terms and categories, filters and default policies.

    b. Set interface language:
        i. Select **Interface** and press **Enter**.

ii. Specify the desired language and click **OK**.

The Management console will be installed in selected language.

c. Click **Accept**.

d. In the opened window make sure the selected languages for pre-installed settings and interface are specified correctly, then click **Yes**.

12. Set parameters of automatic events deletion from DB.
Select one from three options, then click **Select**:

- **Events cleaning** – sets enabling and disabling the automatic deletion of two event types (disabled by default ).
To select the option set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared:
  - **Violation** – enables automatic deletion of events which violate the security policy (see details on policies in "InfoWatch Traffic Monitor. User Guide")
  - **Non-violation** – enables automatic deletion of events which do not violate the security policy of the company.
You can select both items to delete both violating and not violating events.

  Click **Ok**.
- **Violation** – sets a number of days after which event with violations will be deleted from the DB (default: 90 days).
Enter the period of deletion, in days. Click **Ok**.
- **Non-violation** – sets a number of days after which event without violations will be deleted from the DB (default: 45 days).
Enter the period of deletion, in days. Click **Ok**.

  When all settings are set, click **Save settings**.

The installation of the DBMS and a DB scheme will start. The progress of both processes will be displayed on a screen.

The process may take some time.

During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where xxxxxxxxxxxxxxx is the Serial Number of a server.

Web-console installation is performed in an automatic mode. After the completion of the server-end installation the Management console is available through a browser: enter the URL of the Traffic Monitor Server.

The procedure of the further System configuration is described in the document «*InfoWatch Traffic Monitor. Administration Guide*»

## 3.3.2 Installing Traffic Monitor Server (TME Node Server)

**Warning!**

This chapter contains instructions without detailed description of installation screens. For additional information, see «General Information on Installation Steps».

**To install Traffic Monitor Server perform the following steps:**

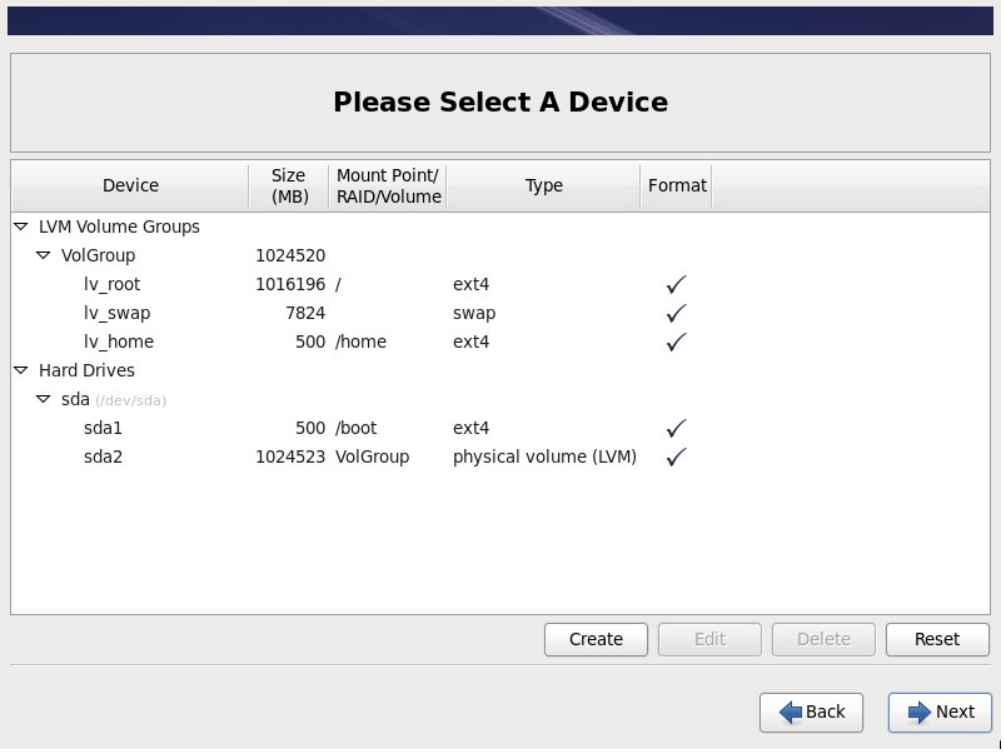
1. Connect the distribution disk: the installation program (kickstart) will run automatically.
2. In the Welcome window, select **TM Enterprise**. Then press **Enter**.
3. In the window of the Database selection, select the required DBMS:
   - **Oracle**
   - **PostgreSQL**

   Then press **Enter**.
4. In the window of installation mode selection, choose **TME Node server** and press **Enter**.

**Warning!**

When the installation mode is selected, the following warning message may appear: «*The storage device below may contain any data*». To clean the disk and start the installation, chick **Yes, discard any data** and leave the field **Apply my choice to all devices with undetected partitions of file systems** unchanged.

5. Specify time zone settings for a server (if the system time is set by Greenwich (UTC), select the field **System clock uses UTC**) and click **Next**.
6. Specify a password for *root* superuser and click **Next**. Recommendations on password creation are available in Appendix A.
7. Specify the mode of disk space partitioning (detailed description see in "Choosing a Disk Partitioning Method"):
   a. Select **Use All Space**.
   b. Select the **Review and modify partitioning layout** checkbox.
   c. Click **Next**.
   d. In **Please Select A Device** window select **lv_home** partition and click **Edit**.
   e. In **Size (MB)** field specify **5000**. Click **OK**.
   f. In **Please Select A Device** window select **lv_root** partition and click **Edit**.
   g. In **Size (MB)** field specify all remain free space (displayed under the field - **Max size is...**). Click **OK**.




h. Click **Next**.

> **Note:**
>
> The **Format > Warnings** window can be displayed which informs you that hard disk partitions, which will be used for installation, need formatting. To continue the installation, click **Format** .

8. The disk partitioning and operating system installation will start. Progress will be displayed on a screen.
   The process may take some time.

   When installation of the operating system is completed, the system will be restarted and you will be prompted to configure network parameters.
9. Configure parameters of a network card and DNS as described in "Network Settings". Click **Save&Quit**.
10. Check specified network settings. If they are incorrect, type **N** and specify correct parameters (see previous steps). If the settings are correct, type **Y** to confirm and press **Enter**.
11. Specify the server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field and press Space, then click **OK**.
12. Specify IP address of the database server and press **Enter**.

**Note:**

If you are using DHCP, it is necessary to tie issuing a certain IP-address to the MAC-address.

13. Check specified network settings. If they are incorrect, type **N** and specify correct parameters. If the settings are correct, type **Y** to confirm and press **Enter**.

During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where `xxxxxxxxxxxxxxx` is the Serial Number of the server.

Web console installation is performed in automatic mode. After the completion of the server-end installation the Management console is available through a browser: enter the URL of the Traffic Monitor Server.

The procedure of further System configuration is described in the document «*InfoWatch Traffic Monitor. Administration Guide*».

## 3.4 Installation of TM Appliance Standard and TM Appliance Enterprise

Installing the IWTM Appliance completely removes all the information (settings, intercepted analysis data, results, etc.) from the server, partitions hard disk, reinstalls an operating system and installs the InfoWatch Traffic Monitor Appliance with default settings.

**Warning!**

This article contains the instruction steps without screenshots and detailed options description. For additional information see «General Information on Installation Steps».

**To install or reinstall IWTM Appliance, execute following steps:**

1. Connect a distributive disk: an installer program (**kickstart**) will start automatically.
2. In the welcome window select:
   - **TM Enterprise** – for installing the Enterprise edition;
   - **TM Standard** – for installing the Standard edition.
3. In the database selection window specify which DBMS should be installed:
   a. Oracle (Standard or Enterprise depending on the edition selected at the previous step);
   b. PostgreSQL.

   Click **Enter**.

4. In the window of installation mode selection, choose **TME Appliance** or **TMS Appliance** (depending on a edition selected in previous step).
5. There is a disk partitioning for Enterprise edition available: a request will be displayed: **Use automatic disc partitioning? (y/n)**.
   Click **y** on a keyboard to make a partitioning according to default parameters.
   If you will click **n** than in several steps you will be suggested to customize partitioning of the disk space.

> **Warning!**
>
> A warning can be displayed: «*The storage device below may contain data*». To clean a disk and start installation, click **Yes, discard any data** and left unchanged the field **Apply my choice to all devices with undetected partitions of file systems**.

6. Specify time zone settings for the server (if the system time is set by Greenwich (UTC), place select the field **System clock uses UTC**) and click **Next**.
7. Specify a *root* superuser password then click **Next**.
   If the entered password does not match with the security rules, a **Weak Password** warning will be displayed. Use buttons:
   - **Use anyway** – if you want to use an entered password without taking recommendations into account
   - **Cancel** – if you want to change the entered password.

   The recommendations on passwords are listed in Appendix A.

   The process may take some time.

   After the completion of operating system installation the computer will be rebooted and you will be suggested to set an address of a time synchronization server (NTP-server).
8. Specify the mode of disk space partitioning:
   a. select **Use All Space**;
   b. click **Next**.

      This step will be skipped if the Standard edition is installing or in step 5 you have selected the auto partitioning of the disk space.

> **Note:**
>
> A **Format Warnings** dialog can be displayed which informs that the formatting of hard disk partitions which will be used for installation is required. To continue the installation click **Format**.

      The disk partitioning and operating system installation will start. The progress of both processes will be displayed on a screen.
9. Specify the address of time synchronization server and click **Ok**. If NTP server cannot be specified for some reasons, click **Cancel** and set this parameter later (details on configuring the NTP server see in "*InfoWatch Traffic Monitor Appliance. Administrator Guide*").

10. Set localization settings:
    a. Specify language of pre-installed entities:
        i. Select **CFDB**, click **Enter**.
        ii. Select required language, click **OK**.
        The pre-installed entities (terms and categories, filters, default policies) will be created in this language.
    b. Specify interface language:
        i. Select **Interface**, click **Enter**.
        ii. Select required language, click **OK**.
        The Managenent Console will be installed with this language.
    c. Click **Accept**.
    d. In the opened window make sure the selected languages for classification settings and interface are specified correctly, then click **Yes**.
11. Set parameters of automatic deletion of events from DB.
    Select one of three options then click **Select**:
    - **Events cleaning** – sets enabling and disabling the automatic deletion of two event types (disabled by default).
      To select the option set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared:
        - **Violation** – sets frequency of automatic deletion of events which are the violation (default: 90 days). See details on violations in «*InfoWatch Traffic Monitor. User Guide*»)
        - **Non-violation** – enables automatic deletion of events which do not violate the security policy of the company.
          You can select both items to delete both violating and not violating events.

      Click **Ok**.
    - **Violation** – sets frequency of automatic deletion of events which are violations (default: 90 days).
      Set frequency of deletion in days. Click **Ok**.
    - **Non-violation** – sets frequency of automatic deletion of events which are not violations (default: 45 days).
      Set frequency of deletion in days. Click **Ok**.
12. After configuring click **Save settings**.

The installation of the DBMS and a DB scheme will start. Progress of both processes will be displayed on a screen.

The process may take some time.

As a result of installation the accounts will be created in a system: see details in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where `xxxxxxxxxxxxxxx` is the Serial Number of a server.

Web-console installation is performed in an automatic mode. After the completion of the server-end installation the Management console is available through a browser: enter the URL of the Traffic Monitor Server.

A further System configuration is described in "*InfoWatch Traffic Monitor. Administrator Guide*".

## 3.5 Installing the Crawler Subsystem

Crawler interceptor is implemented as two Windows services:

- `InfoWatch.Crawler.Scanner` – scans network folders and file storages according to settings configured by user;
- `InfoWatch.Crawler.Server` – manages scanning service and enables communication with Traffic Monitor Management Console.

**Warning!**

For interaction with one database schema, **only one** instance of Crawler server can be used. One Crawler server can interact with **only one** instance of Crawler scanner.

Before installation, please read software and hardware requirements for computers where System components will be installed. Both components of Crawler subsystem (server and scanner) are installed from the same distribution.

**Warning!**

Both Crawler server and Crawler scanner must be installed on computers located in the same domain: the one which contains all the computers that will be scanned.

**To install Crawler:**

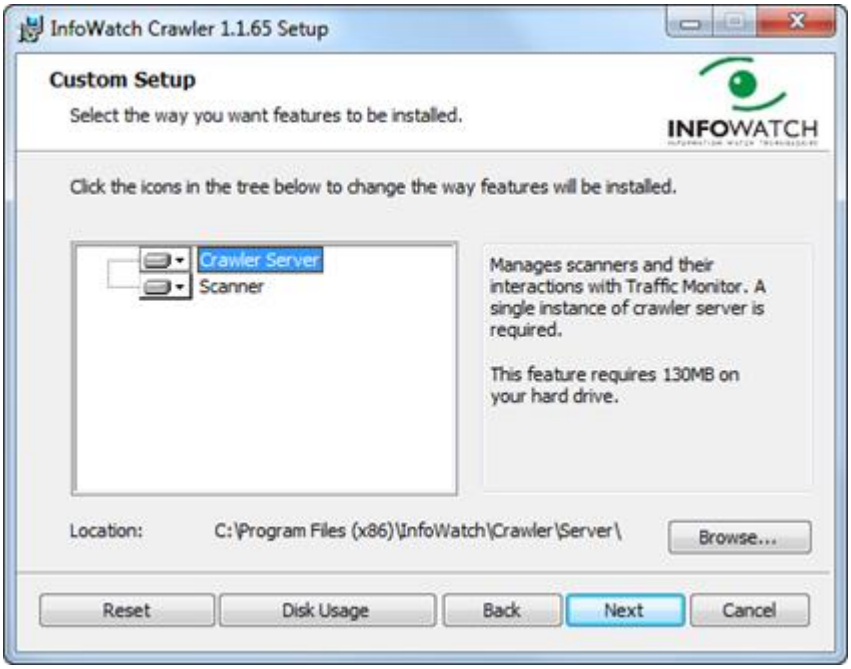
1. Run `Crawler_vx.x.x.xxx.msi` installation package, where x.x.x.xxx is a version number.

**Note:**

The language of the Installation Wizard is defined automatically and depends on the selected format (see **Start -> Control Panel -> Region and Language**, **Formats** tab).

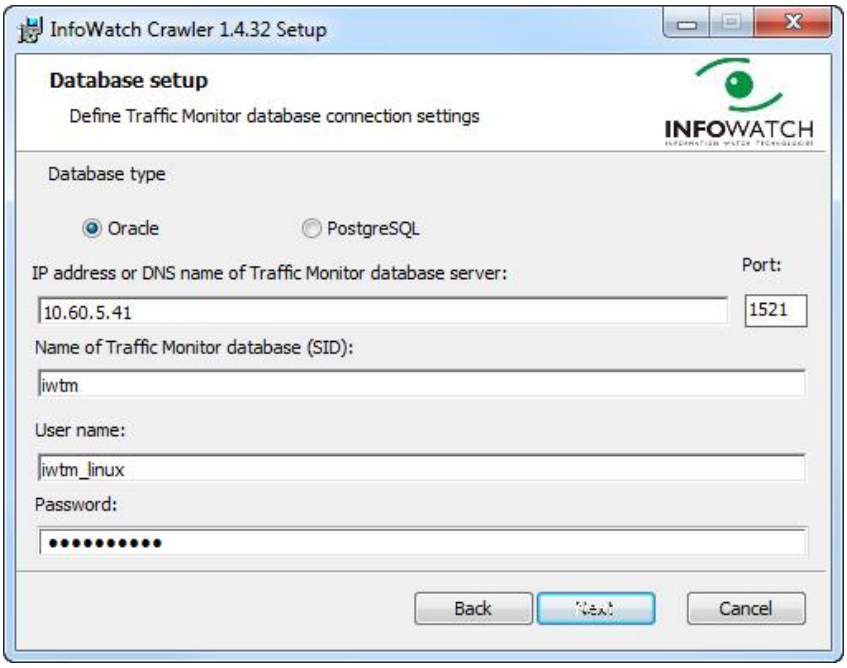
2. In the Welcome screen of InfoWatch Crawler Installation Wizard, click **Next**.
3. In the Installation Scope screen, click **Next**.

4. At the **Custom Setup** step, specify which Crawler components should be installed and choose the installation directory:
   - **Server Crawler** – installing the `InfoWatch.Crawler.Server` service that manages scanning tasks and provides communication with the server, database and Traffic Monitor Management Console.
   - **Scanner component** – installing the `InfoWatch.Crawler.Scaner` service that scans network folders and file storages according to the settings configured by a user.




   If you do not want to install a particular component, click on this feature and select ✕ **Entire feature will be unavailable**.
   Specify paths to the directories where selected components will be installed and click **Next**.

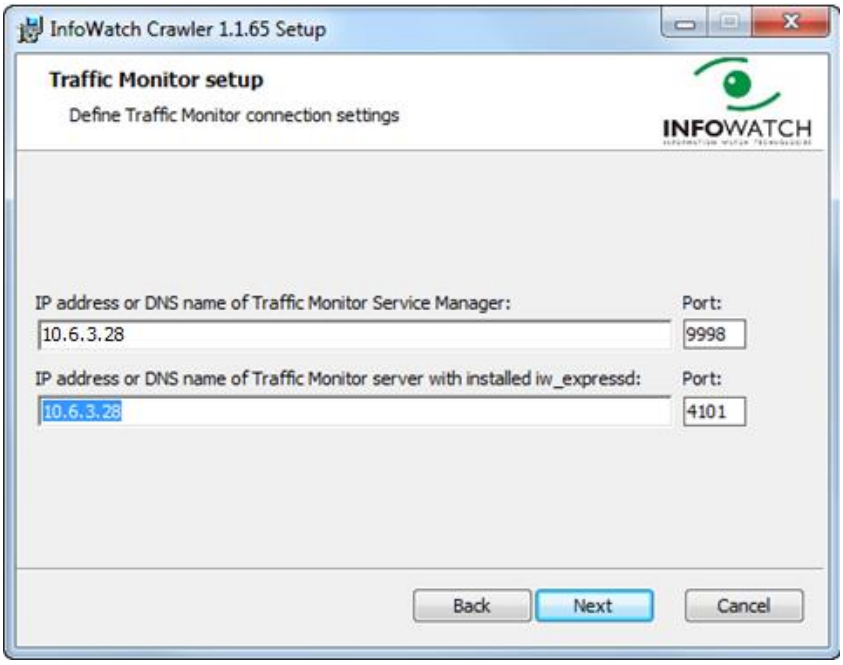
5. If at the **Custom Setup** step, you have chosen the **Server Crawler**:
   a. Specify parameters for connection of the `InfoWatch.Crawler.Server` service with Traffic Monitor database, click **Next**.




Depending on used DBMS, connection settings may vary:

| Setting | Oracle | PostgreSQL | Notes |
|---|---|---|---|
| IP address or DNS name | According to the TM DB server in use | | |
| Port | 1521 | 5433 | |
| Database name | iwtm | postgres | The PostgreSQL needs SID or service name. |
| Username | iwtm_linux | iwtm_linux | User of the Linux part of DBMS on behalf of which the intercepted events will be downloaded to the database. |
| Password | xxXX1234 | xxXX1234 | If was not changed after Traffic Monitor server part installation. |

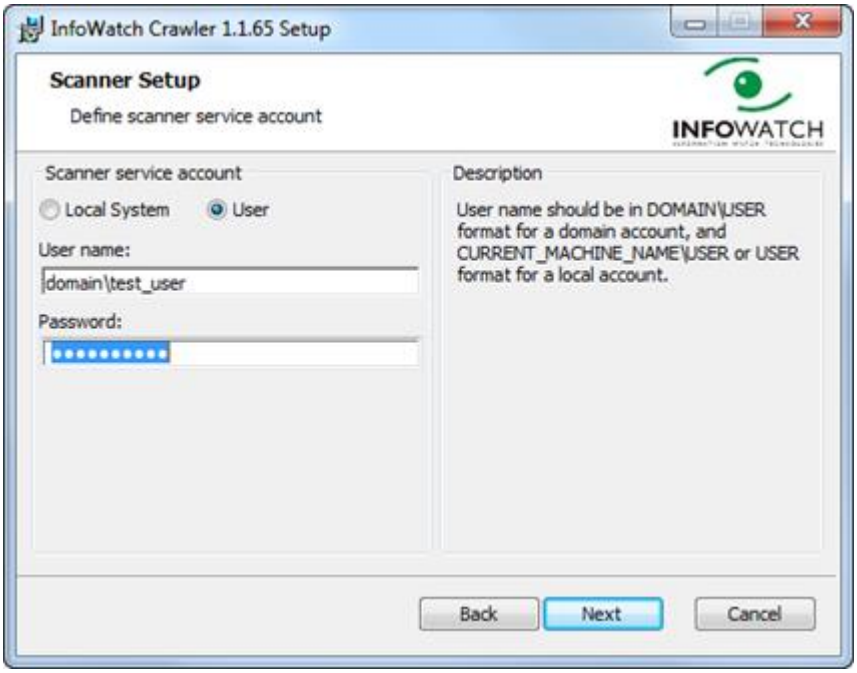
b. Specify parameters for connection of the `InfoWatch.Crawler.Server` service with Traffic Monitor server, click **Next**.




In case of distributed installation, specify the following values:
- in the **IP address or DNS name of Traffic Monitor Service Manager** field, specify the IP address of the TM DB server
- in the **IP address or DNS name of Traffic Monitor server with installed iw_expressed** field, specify the IP address of the TME Node Server.

6. If on the **Custom Setup** step you have chosen the installation of **Scanner component**:

   a. specify an account that will be used to launch `InfoWatch.Crawler.Scaner` service. You can select a standard Local System account (recommended) or specify an account which has permissions for running services in the background mode (this option is configured in **Panel –> Administrative Tools –> Local Security Policy –> local policies –> User Rights Assignment –> Log on as a service**). Click **Next**.



b. specify:
   - IP address or DNS name of the computer where the **Server** component is installed;
   - port number of the Crawler server;
   - path to the directory where the Scanner will temporary store files that are copied from checked resources.

> **Note:**
> If the **Temporary files directory** field is left blank then the installer will automatically select the last path value used in the operating system.

7. Click **Next**.
8. Click **Install** to start the installation. When the installation is complete, click **Finish**.
9. After installation of the Crawler server, start it with the following steps:
   a. go to the server where **iwtm-webgui** package is installed;
   b. in the **web.conf** file, change the value of the `kickers.crawler` parameter from "0" to "1";
   c. execute the command: `service iwtm restart kicker`.

# 3.6 Pre-installed Server Settings

The installation of a server part of the System is installed creates a set of entinies which can be referred lately while configuring and maintaining the System.

The hostname is **iwtm-xxxxxxxxxxxxxxxx.local** where xxxxxxxxxxxxxxxx is a Serial Number of the server.

System installation directories (can be placed on different servers):

- Traffic Monitor server – **/opt/iw**
- DB – **/u01** and **/u02**

> **Note:**
> When installing Traffic Monitor version `6.1.100` or earlier, DB PostgreSQL is installed only to `/u01` directory.

Settings of the Traffic Monitor database:

| Settinng | Oracle | PostgreSQL |
|---|---|---|

| | | |
|---|---|---|
| DB connection port | **1521** | **5433** |
| DB name / SID or service name | **iwtm** | **postgres** |

Accounts:

| **Account** | **Name** | **Password** |
|---|---|---|
| Superuser of Linux OS (root) | root | Specified during installation |
| Linux user on whose behalf the Traffic Monitor server processes will be run | iwtm | no password |
| Oracle administrator | sys | xxXX1234 |
| | system | xxXX1234 |
| Database scheme owner | iwtm | xxXX1234 |
| User of the DBMS Linux part on whose behalf the intercepted objects will be loaded to a database | iwtm_linux | xxXX1234 |
| User on whose behalf the Web interface will interact with DB | iwtm_web | xxXX1234 |
| Management Console user administrator | administrator | xxXX1234 |
| Management Console security officer | officer | xxXX1234 |
| Linux user on whose behalf the DB server processes will be run<br>**Warning!** It is strongly recommended to change the account password immediately after the installation completion . | oracle | xxXX1234 |

Group of owner of the Oracle DBMS Client installation which includes iwtm and oracle users - **oinstall**

# 4 UPDATING THE SYSTEM

**Warning!**

IWTM Appliance allows to update the System in a simplfied way: through the Management Console. See details in the Administrator Guide, "*System Update of the Traffic Monitor Appliance*" article.

**To update the System for the "All-in-one" installation mode**:

1. Update RHEL and IWTM packages.
2. Update DB schema for Oracle or PostgreSQL.
3. Reboot the server.

**To update the System for the distributed installation type**:

1. On TM and DB server update RHEL and IWTM packages.
2. On DB server, update DB schema for Oracle or PostgreSQL.
3. Reboot database server.
4. Reboot Traffic Monitor server.

Before starting an update process, check whether `/opt/iwks_mode` file is present in the system and installation type specified in this file matches the actual installation type.
The file may contain the following parameters:

| Parameter | Value |
|---|---|
| iwall | All components of the InfoWatch Traffic Monitor Enterprise are installed on the same computer |
| iwtm | Installing Traffic Monitor Server to a separate computer |
| iwdb | Installing DBMS Server with a Traffic Monitor database schema to a separate computer |
| iwtms | All components of the InfoWatch Traffic Monitor Standard are installed on the same computer |
| apple | InfoWatch Traffic Monitor Appliance Enterprise |
| appls | InfoWatch Traffic Monitor Appliance Standard |

If the file is missing or contains incorrect installation version, create this file and/or specify the correct parameter.

**Warning!**

In the updating the system.lua configuration file is replaced, so the System operates in default transport mode - the copy mode. If you need to use the blocking mode (in-line) then in the

конфигурационном файле **system.lua** configuration file please replace **Copy** value of the **transport_mode** setting with **Normal** one. Details on configuring the transport mode see in the Administrator Guide, "Configuring Traffic Interception" section, see subsection for each needed traffic type.

.

# 4.1 Updating RHEL and IWTM Packages

To update the System, you need to connect **kickstart**. Packages required for update are installed from this disk.

1. In any partition of a hard drive, create a directory and mount the CD:
   `mkdir /mnt/rhel-dvd && mount /dev/cdrom /mnt/rhel-dvd`
2. In the `/etc/yum.repos.d` directory, create a **rhel-dvd.repo** file (this file is required for specifying paths to update packages).
3. Open the **rhel-dvd.repo** file for editing and insert the following text:

```
[rhel-dvd]
 name=Red Hat Enterprise Linux $releasever - $basearch - DVD
 baseurl=file:///mnt/rhel-dvd/
 enabled=1
 gpgcheck=0

[rhel-dvd-iwtm]
 name=Red Hat Enterprise Linux $releasever - $basearch - DVD
 baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux
 enabled=1
 gpgcheck=0
```

4. Save changes in the **rhel-dvd.repo**.
5. Clean up the package manager cash:
   `yum clean all`
6. Delete the `iwtm-tmcap`:

   `rpm -e --nodeps iwtm-tmcap`

   **Warning!**

   Otherwise the tmcap.ko cernel module can be deleted during the update process and reinstalling of the `iwtm-tmcap`.

   When updating a database server, deleting the `iwtm-tmcap` is not required.

7. Install `kernel-headers` of the actual kernel version:

   `yum install kernel-headers`

> **Note:**
>
> If no changes have been made to kernel-headers after installation of the System, skip this step.

8. Install the `iwtm-tmcap`:

   ```
   yum install iwtm-tmcap
   ```

9. Run packages update process:
   ```
   yum update
   ```

10. Check if there are new versions of configuration files with **conf.rpmnew** extention in the directory `/opt/iw/tm5/etc/`**.**
    - If yes, align them with the old configuration files.
11. Check if there are new versions of Nagios configuration files with **cfg.rpmnew** extention in the directory `/etc/nagios/iwmon`**.**
    - If yes, align them with the old configuration files.
12. If the **config_manager.conf**configuration file has been modified in the previous version, then copy the settings from the Serman section of the **config_manager.conf.rpmsave** file to the `Serman` section of the **agent.conf**. Both files are located in the `/opt/iw/tm5/etc`.

## 4.2 Updating the Oracle Database Schema

1. Connect to the database on behalf of the schema owner
   ```
   su - oracle
   sqlplus
   ```

> **Note:**
>
> Default login of the schema owner is `iwtm` .

2. Disconnect users from the database.
3. Stop services that may have access to database:
   ```
   service iwtm stop
   service php-fpm stop
   service nagios stop
   ```

> **Note:**
>
> In case there is Crawler subsystem installed in the System, the processes of this subsystem on the Crawler Server must be stopped.

4. Make sure that the **database.conf** configuration file located in directory `/opt/iw/tm5/csw/oracle`has been updated correctly and contains an actual version of database schema.
5. Go to directory `/opt/iw/tm5/csw/oracle`:

   ```
   cd /opt/iw/tm5/csw/oracle
   ```

6. Run database update with a script:
   ```
   ./update.sh
   ```
7. Start the stopped services:
   ```
   service iwtm start
   service php-fpm start
   service nagios start
   ```

> **Note:**
>
> In case there is Crawler subsystem installed in the System, the processes of this subsystem on the Crawler Server must be stopped.

8. Apply the configuration in the Management console (see details in "*InfoWatch Traffic Monitor. User Guide"*).

## 4.3 Updating the PostgreSQL Database Schema

1. Connect to the database on behalf of the schema owner
   ```
   su postgres
   psql -p 5433
   ```

> **Note:**
>
> Default login of the schema owner is `iwtm`.

2. Disconnect users from the database.
3. Stop services that may have access to database:
   ```
   service iwtm stop
   service php-fpm stop
   service nagios stop
   ```

> **Note:**
>
> In case there is Crawler subsystem installed in the System, the processes of this subsystem on the Crawler Server must be stopped.

4. Make sure that the **database.conf**configuration file located in directory `/opt/iw/tm5/csw/postgres`has been updated correctly and contains an actual version of database schema.
5. Go to directory `/opt/iw/tm5/csw/postgres`:

   ```
   cd /opt/iw/tm5/csw/postgres
   ```

6. Run database update with a script:
   ```
   ./update.sh
   ```
7. Start the stopped services:
   ```
   service iwtm start
   service php-fpm start
   service nagios start
   ```

> **Note:**
>
> In case there is Crawler subsystem installed in the System, the processes of this subsystem on the Crawler Server must be stopped.

8. Apply the configuration in the Traffic Monitor Management console (see details in "InfoWatch Traffic Monitor. User Guide").

# 5 UNINSTALLING THE SYSTEM

The System uninstalling implies the deletion of all packages of the System as well as removal of a used database scheme. To completely delete the operating system and the DBMS you, for example, can execute formatting of used partitions by standard tools.

- See details on DB schema removal (Oracle as well as PostrgreSQL) in "Deleting the Database Scheme".
- The Crawler subsystem (server as well as scanner) can be removed by standard OS Windows tools: **Start -> Control panel -> Programs and components**, a **Delete** command.
- To delete a certain package, execute a command:

  ```
  rpm -e package_name
  ```
- ```
  All the Traffic Monitor server components (Management console, Sniffer, IW ICAP, remote database interaction module, and the others) can be deleted by the following command:
  yum remove `rpm -qa | grep iwtm`
  ```

After the InfoWatch Traffic Monitor Server removal completion please return the external infrastructure set to Traffic Monitor to original state:

- if there was an integration with a mail relay server – please make sure the Postfix settings are set to original state;
- if the System performed interception and filtering of SMTP traffic – please configure the SMTP mail delivery through a corporate mail server, bypassing the InfoWatch Traffic Monitor server.

After removal there are following entities left on the computer:

- an operating system;
- configuration files where changes were made ( **.rpmsave** suffix is being assigned to the changed files - for example, **detector.conf.rpmsave**; files that was not changed will be deleted);
- objects queue (see details on deletion of files from the OS temporary directory and data from IW Traffic Monitor file queue directories in «*InfoWatch Traffic Monitor. Administrator Guide*», "*Deleting Temporary Files*" article);
- categories and terms;
- license file;
- account of a user which is a IW Traffic Monitor owner and the group to which this user belongs.

## 5.1 Deleting the Database Scheme

This instruction is relevant for the Oracle Database and PostrgreSQL.
  ```

**Warning!**

Do not delete the database scheme from which the daily table spaces were distracted for archiving. Otherwise you will not be able to restore data from these table spaces.

1. **Checking the Oracle DBMS**

   Make sure that:

   - the version of a installed database scheme corresponds to a version of a software package used for its removal;
   - the DBMS server is running;
   - in configuration file **database.conf** the name and the password of account having SYSDBA permissions are specified correctly (values of parameters `sysdba` and `sysdba_password`).

2. **Stopping the TrafficMonitor**

   a. Stop all TM server processes:
   `service iwtm stop`

   b. Close all copies of the Management console;

   c. Stop the web service:
   service php-fpm stop

   d. Stop all the connections with a database scheme executed from other programs.

3. **Starting the schema removing**

   a. Go to directory
   `/opt/iw/tm5/csw/oracle` or `/opt/iw/tm5/csw/postgres`

   b. Run script:
   ./uninstall.sh

**Warning!**

Plugins and tokens are deleted from System when deliting DB scheme (see "Infowatch Traffic Monitor 6.0. Administration guide", article "Plugins"). To reestablish Device Monitor plugin:

1. Create **/opt/iw/tm5/www/backend/protected/runtime/first_run** file using **iwtm** user;
2. Restart **iw_kicker** process:
   `service iwtm restart kicker`

It is required to add other plugins manually (see "Infowatch Traffic Monitor 6.0. Administration guide", article "Adding plugin").

## 5.2 Crawler

Crawler subsystem (both **Server** and **Scanner**) can be deleted using standard Windows tools: **Start -> Control Panel -> Programs and components**, the **Delete** command.

# 6 APPENDIX A. USERNAME AND PASSWORD RECOMMENDATIONS

**Requirements for usernames**

- The user name should be 1-20 characters long.
- The user name may include English letters, digits and underscore "_". Must begin with a letter.

**Requirements for passwords**

- The user password should be 1-30 characters long..
- The user password may include English letters, digits, and also the following characters: «#», «$» или «_».
  Must begin with a letter.

- The password is case-sensitive.

**Recommendations for strong passwords**

- Recommended password length is 10-30 characters.
- The password must contain letters, digits and characters.
- It is not advised to:
  - Include whole words or phrases into a password.
  - Use a series of the same character.
  - Start and end the password with the same character.
  - Create a new password by adding characters to your current password.

**General recommendations**

It is not recommended beginning a username or password with combinations: SYS_ and ORA_.
It is not recommended using Oracle reserved words in usernames or passwords:

| | | | |
|---|---|---|---|
| ACCESS | EXCLUSIVE | MODE | SELECT |
| ADD | EXISTS | MODIFY | SESSION |
| ALL | FILE | NOAUDIT | SET |
| ALTER | FLOAT | NOCOMPRESS | SHARE |
| AND | FOR | NOT | SIZE |
| ANY | FROM | NOWAIT | SMALLINT |
| AS | GRANT | NULL | START |
| ASC | GROUP | NUMBER | SUCCESSFUL |

| | | | |
|---|---|---|---|
| AUDITBETWEEN | HAVING | OF | SYNONYM |
| BY | IDENTIFIED | OFFLINE | SYSDATE |
| CHAR | IMMEDIATE | ON | TABLE |
| CHECK | IN | ONLINE | THEN |
| CLUSTER | INCREMENT | OPTION | TO |
| COLUMN | INDEX | OR | TRIGGER |
| COMMENT | INITIAL | ORDER | UID |
| COMPRESS | INSERT | PCTFREE | UNION |
| CONNECT | INTEGER | PRIOR | UNIQUE |
| CREATE | INTERSECT | PRIVILEGES | UPDATE |
| CURRENT | INTO | PUBLIC | USER |
| DATE | IS | RAW | VALIDATE |
| DECIMAL | LEVEL | RENAME | VALUES |
| DEFAULT | LIKE | RESOURCE | VARCHAR |
| DELETE | LOCK | REVOKE | VARCHAR2 |
| DESC | LONG | ROW | VIEW |
| DISTINCT | MAXEXTENTS | ROWID | WHENEVER |
| DROP | MINUS | ROWNUM | WHERE |
| ELSE | MLSLABEL | ROWS | WITH |

# 7 APPENDIX B. LICENSES FOR THIRD-PARTY TECHNOLOGIES

System contains third-party components distributed under MIT License (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

The System also uses software:

- Distributed under BSD license (http://www.opensource.org/licenses/bsd-license.php):
  - Stringencoders – http://code.google.com/p/stringencoders/
- Distributed under GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
  - Pdftotext – http://www.foolabs.com/xpdf/
  - Tnef – http://sourceforge.net/projects/tnef/
  - Unzip – http://www.info-zip.org/UnZip.html
  - libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
  - libhtmltree.so – pauljlucas@mac.com