

INFOWATCH

InfoWatch Traffic Monitor 6.5

Installation Guide

InfoWatch Traffic Monitor 6.5

Installation Guide

© AO “InfoWatch”

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

http://www.infowatch.com

Revision date: 2016-08-31

TABLE OF CONTENTS

1 INTRODUCTION 5

1.1 WHO SHOULD READ THIS GUIDE 5
1.2 SET OF DOCUMENTS 5
1.3 TECHNICAL SUPPORT 5

2 GETTING READY TO INSTALL 7

2.1 SYSTEM DEPLOYMENT SCHEMES AND INSTALLATION TYPES 7
2.2 DEPLOYMENT SCHEME FOR INFOWATCH DEVICE MONITOR 9
2.3 HARDWARE AND SOFTWARE REQUIREMENTS 11

3 INSTALLING THE SYSTEM 19

3.1 GENERAL INFORMATION ON INSTALLATION STEPS 20
3.1.1 Start Window 21
3.1.2 Selecting the Database 22
3.1.3 Selecting the Installation Mode 22
3.1.4 Choosing a Time Zone 23
3.1.5 Setting Password for System Superuser 24
3.1.6 Choosing a Disk Partitioning Method 24
3.1.7 Network Settings 28
3.1.8 Configuring Time Synchronization (NTP-server) 31
3.1.9 Localization Setting 32
3.1.10 Configuring the Automatic Event Deletion from the Database 34
3.1.11 Completing the Installation 35
3.2 ALL-IN-ONE INSTALLATION MODE OF TM ENTERPRISE AND TM STANDARD 36
3.3 DISTRIBUTED INSTALLATION OF TM ENTERPRISE 41
3.3.1 Installing Database (TM DB Server) 42
3.3.2 Installing Traffic Monitor Server (TME Node Server) 45
3.4 INSTALLING THE CRAWLER SUBSYSTEM 47
3.5 PRE-INSTALLED SERVER SETTINGS 51
3.6 INSTALLING INFOWATCH DEVICE MONITOR 52
3.6.1 InfoWatch Device Monitor Server End Setup 53
3.6.1.1 Database deployment under Microsoft SQL Server DBMS 53
3.6.1.2 Database deployment under Oracle DBMS 54
3.6.1.2.1 Configuring InfoWatch Device Monitor connection to Oracle DBMS server 54
3.6.1.3 Server Setup Recommendations 55
3.6.1.4 Server End Installation Procedure 56
3.6.2 InfoWatch Device Monitor Client Installation 63
3.6.2.1 Standard Client Installation 64
3.6.2.2 Client Installation via Software Distribution Tools 65

4 UPDATING THE SYSTEM 69

4.1 UPDATING RHEL AND IWTM PACKAGES 70
4.2 UPDATING THE ORACLE DATABASE SCHEMA 71
4.3 UPDATING THE POSTGRESQL DATABASE SCHEMA 72
4.4 UPDATING INFOWATCH DEVICE MONITOR 73
4.4.1 Updating InfoWatch Device Monitor Server End 74
4.4.1.1 Step 1. Start update 74
4.4.1.2 Step 2. Accepting the License Agreement 74
4.4.1.3 Step 3. Database configuration 74
4.4.1.4 Step 4. Upgrade Completion 75
4.4.2 Updating InfoWatch Device Monitor Client 75

5 UNINSTALLING THE SYSTEM 77

5.1 DELETING THE DATABASE SCHEME 77
5.2 CRAWLER 79
5.3 UNINSTALLING INFOWATCH DEVICE MONITOR 79
5.3.1 Remove Client Installed via Software Distribution Tools 80

6 APPENDIX A. USERNAME AND PASSWORD RECOMMENDATIONS 82

7 APPENDIX B. LICENSES FOR THIRD-PARTY TECHNOLOGIES 84

1 INTRODUCTION

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

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, the database in use (Oracle / PostgreSQL), and the edition (Standard / Enterprise).

The following typical solutions can be:

- **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.

> **Note:**
>
> You should not install or run applications (especially server ones) on Traffic Monitor or Database server or use it 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 PostgreSQL
Storage period of intercepted data	Limited by storage size only		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!

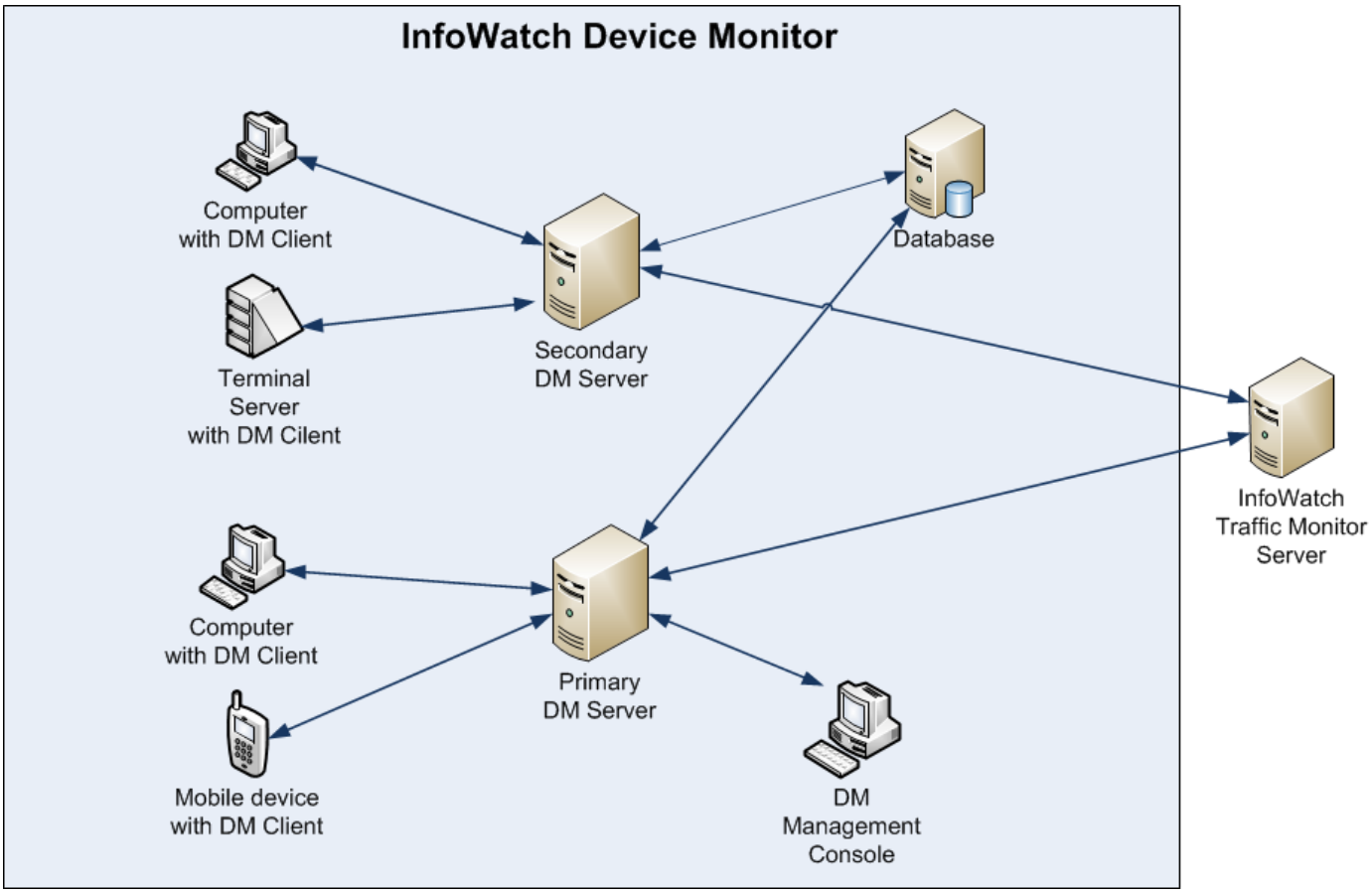
After installation, the Administrator configures the System depending on implementation purposes (see "*InfoWatch Traffic Monitor. Administration Guide*", "Configuring the System after Installation").

2.2 Deployment Scheme for InfoWatch Device Monitor

InfoWatch Device Monitor components are listed in the following table:

Component	Purpose
InfoWatch Device Monitor Client (InfoWatch device monitor client application, Client)	Intercepting employees' actions on controlled computers and mobile devices
InfoWatch Device Monitor Server (InfoWatch device monitor server, Server)	Configuring client applications, retrieving data from client applications and sending it to InfoWatch Traffic Monitor
InfoWatch Device Monitor Database (database)	Storing data which is required for the operation of Device Monitor
InfoWatch Device Monitor Management Console (Management Console)	Managing Device Monitor
Servers Manager	Configuring roles and other attributes of Device Monitor servers

The following image illustrates interaction of Device Monitor components:



You can use clustering to enhance the performance. The same database schema will be used by multiple servers to store and distribute shared security schema.

Server and database can be hosted on a single computer. To increase the performance, it is recommended that you should host the database and server on separate computers.

The Management Console can only connect to the main server. From the Management Console, you can manage all servers in the cluster.

InfoWatch DeviceMonitor is deployed and works as follows:

1. The **primary server** is installed first (see the document "*Infowatch Traffic Monitor. User Guide*", "InfoWatch Device Monitor Server Manager" article).
2. When you install the primary server, you should specify the server that will be used by the **database**: DBMS can be stored separately or together with the primary server.
3. During installation of the primary server, a **database schema** is created, where the **security schema** and other Device Monitor parameters are stored.
4. You can install **secondary servers**, if needed, to balance the workload.
5. The **Management Console** can be installed on any computer. It connects to the primary server. The Management Console is used for configuring the security scheme according to the corporate security policy.
6. **Device Monitor Clients** are installed on **workstations** and **mobile devices**. Clients connect to any available Device Monitor Server via an encrypted channel with binding to the Server by the key, which is used for traffic encryption. Device Monitor clients ensure implementation of security schemes; they also retrieve shadow copies and send them to Device Monitor Server.
7. Device Monitor Server retrieves updated versions of the security scheme from the database and distributes them to controlled workstations and mobile devices. Information about events that subject to a security scheme rule and files shadow copies are sent from tThe controlled workstations and mobile devices to the Server. Information about the events is sent to the database. Shadow copies are sent to InfoWatch Traffic Monitor.

Example 1

1. An employee who works at a controlled workstation tries to get access to a controlled peripheral (for example, attempts to print a document on a USB printer).
2. The Client checks if the employee has permissions to access the peripheral. If not, access is denied (in this case, the document wil not be printed).

Printing operations on local and network printers are monitored by Print Monitor interceptor. Print task copies are sent to InfoWatch Monitor Traffic for analysis. Employees can print documents, only if they are allowed to access the printer (this is checked by Device Monitor interceptor).

Example 2

There is a rule in Device Monitor that monitors writing to PDF files on a removable device. According to the rule, during this operation, a shadow copy of the document is created.

1. An employee who works at a controlled workstation writes data to a file on a removable device (for example, copies a file to USB flash drive).
2. If writing to a removable device is successful, InfoWatch Device Monitor Client generates an event and creates a shadow copy of the file.
3. If the creation of a shadow copy fails (for example, there is no free space on the hard drive), writing to file will be performed without creating a shadow copy (this will be specified in the event data).

4. The Client transmits data (the event and the file shadow copy) to InfoWatch Device Monitor Server. If there is not connection to the Server, the data is stored on the computer. Once the connection is restored, the data will be sent to Server.
5. The Server sends data to InfoWatch Traffic Monitor for analysis. If no there is no connection to InfoWatch Traffic Monitor server, the data is stored on the computer. Once the connection is restored, the data will be sent to InfoWatch Traffic Monitor.

Any attempts to write to files on removable devices are monitored by File Monitor interceptor. Obtained data is then passed to InfoWatch Traffic Monitor for analysis. At the same time, access to removable devices is controlled by Device Monitor interceptor. Therefore, employess can write data to file on a removable device only if they have access to the device.

Example 3
There is a rule in Device Monitor that monitors DOC files. According to the rule, during this operation, a shadow copy of the document is created.

1. An employee who works at a controlled workstation sends a document to print.
2. If the print job is created successfully, InfoWatch Device Monitor Client generates an event and creates a shadow copy of the printed document.
3. If the creation of a shadow copy fails (for example, there is no free space on hard drive), print operation will be performed without creating a shadow copy (this will be specified in the event data).
4. The Client transmits data (the event and the file shadow copy) to InfoWatch Device Monitor Server. If there is not connection to the Server, the data is stored on the computer. Once the connection is restored, the data will be sent to Server.
5. The Server sends data to InfoWatch Traffic Monitor for analysis. If no there is no connection to InfoWatch Traffic Monitor server, the data is stored on the computer. Once the connection is restored, the data will be sent to InfoWatch Traffic Monitor.

2.3 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 edtion. 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 the 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	RAID-array with fault tolerance: 300 GB	2CPU 6xC, 2,6 GHz	24 GB	No requirements: the kickstartinstallatorformats the hard drive and installs all required software.	Traffic Monitor server can use interceptors which raise additional requirements: • **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). • **iw_icap** handles ICAP client built in any proxy server confirming RFC 3507 standard (for example SQUID 3.4.x
TM Enterprise server, less than 10 GB/day	RAID-array with fault tolerance: 600 GB	2CPU 8xC + Hyper-threading (Intel® Xeon® Processor E5-2640 v3 - 2,6 Hz)	24 GB		
TM Enterprise server, from 10 GB/day to 50 GB/day	RAID-array with fault tolerance	2SRVx2CPU 10xC	32-48 GB for each server		

Traffic Monitor element	**Hard disk**	**Processor**	**RAM**	**Software**	Additional requirements
TM Enterprise server, more than 50 GB/day	RAID-array with fault tolerance	Calculated on demand	From 32GB for each server		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. The server should have a network interface with the assigned IP address.
Oracle DB or PostgreSQL server	RAID-array with fault tolerance: 500 GB	2CPU от 6xC, 2,6 GHz	16GB and more depending on data volume,insertionand processing speed		Provides storage for traffic of 1-2 thousand users by 3 months; without OCR, without Device Monitor

Traffic Monitor element	**Hard disk**	**Processor**	**RAM**	**Software**	Additional requirements
Crawler server and scanner	30 GB of free space - for the server and the scanner: required for temporary storage of files that are copied from checked resources and for installation purposes	From 2 cores	From 2 GB	OS: • Microsoft Windows Vista 7/8 SP2 • Microsoft Windows Server 2008 R2 SP1 or SP2/2012 • Microsoft Windows 7 SP1 Platform: • Microsoft .Net Framework 4.5	• **iw_expressd** process autorun should be enabled on the TM server (see details in «*InfoWatch Traffic Monitor. Administration Guide*») • Both Crawler Server and Scanner should be installed on computers located in the same domain which includes all workstations supposed to be scanned. • 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. • 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.

Traffic Monitor element	**Hard disk**	**Processor**	**RAM**	**Software**	Additional requirements
Device Monitor server	Not less than 200 MB free space for installation	From 2 cores	From 2 GB	OS (x86 and x64 platforms are supported): • Microsoft Windows Server 2003; • Microsoft Windows Server 2008; • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2. Platform: • Microsoft .Net Framework 4.0 DBMS client: • Oracle Database 11. If you install Device Monitor on x64 server OS, using x64 Oracle Client application is required. • Microsoft SQL Server 2005, 2008, 2012, 2014 (Express, Developer, Workgroup, Standard, Enterprise). • PostgreSQL version 8 and 9.	• Autostart for **iw_expressd** and **iw_xapi** processed should be enabled on TM server • Local DNS is required to convert domain names into addresses

Traffic Monitor element	**Hard disk**	**Processor**	**RAM**	**Software**	Additional requirements
Device Monitor Agent for workstations	Not less than 320 GB free space for temporary storage of files which are then sent for analysis	From 2 cores	From 2 GB	OS: • Microsoft Windows XP Professional Service Pack 3 with all updates; • Microsoft Windows Vista Service Pack 2; • Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 and 8.1; • Microsoft Windows 10; • Microsoft Windows Server 2003; • Microsoft Windows Server 2008; • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2. Platform: • Microsoft .Net Framework 4.5	Local DNS is required to convert domain names into addresses

Traffic Monitor element	**Hard disk**	**Processor**	**RAM**	**Software**	Additional requirements
Device Monitor Agent for mobile devices	No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	The following device configurations on Android platform are supported: • ASUS Nexus 7 2013 LTE (K009), Android version 4.3.0 (build version JLS36C) • ASUS Nexus 7 2013 LTE (K009), Android version 4.4.2 (build version KOT49H) • ASUS Nexus 7 2013 LTE (K009), Android version 4.4.3 (build version KTU84L) • ASUS Nexus 7 2013 LTE (K009), Android version 4.4.4 (build version KTU84P) • Samsung Galaxy S3 (I9300), Android version 4.3.0 (build version JSS15J.I9300XXUGNK1, JSS15J.I9300XXUGND2) • Samsung Galaxy S4 (I9500), Android version 4.3.0 (build version JSS15J.I9500XXUEMK8) • Samsung Galaxy S4 (I9505), Android version 4.3.0 (build version JSS15J.I9505XXUEMK9, JSS15J.I9505XXUEML4) • Samsung Galaxy S4 (I9505), Android version 4.4.2 (build version KOT49H.I9505XXUGNG8, KOT49H.I9505XXUFNC9) • Samsung Galaxy S5 (SM-G900F), Android version 4.4.2 (build version KOT49H.G900FXXU1ANE2, KOT49H.G900FXXU1ANK7) Devices on iOS platform

Traffic Monitor element	**Hard disk**	**Processor**	**RAM**	**Software**	Additional requirements
Device Monitor Console	Not less than 35 MB	Same as for used OS	Same as for used OS	OS: • Microsoft Windows Server 2003; • Microsoft Windows Server 2008; • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows XP Professional Service Pack 3; • Microsoft Windows Vista Service Pack 2; • Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 and 8.1; • Microsoft Windows 10.	

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 for 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**	• Installing OS Linux • Configuring network interface • Installing and configuring DBMS Oracle (only for **TME All-in-one**) or PostgreSQL • Installing IW Traffic Monitor database schema • Installing RPM packages of IWTM Server • Installing Monitoring subsystem • Installing Management console
DBMS Server with Traffic Monitor DB schema on a separate computer	**TME DB server**	• Installing OS Linux • Configuring network interface • Installing and configuring DBMS Oracle or PostgreSQL • Installing IW Traffic Monitor database schema

Traffic Monitor Server on the separate computer	**TME Node server**	• Installing OS Linux • Configuring network interface • Installing RPM packages of IWTM Server • Installing Monitoring subsystem • 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
- 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;
- 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

> **Important!**
>
> **TM Standard** edition is available only in **TMS All-in-one** mode: **TM+DB server - PostgreSQL**. In this mode, "Selecting the Database" and "Selecting the Installation Mode" steps will be omitted.

- **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



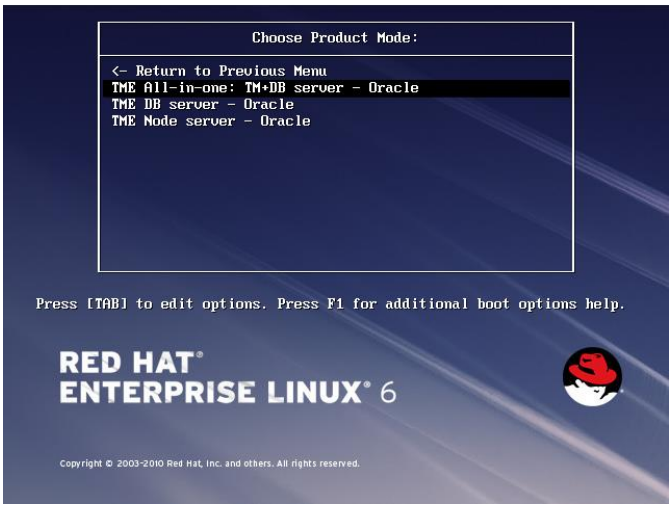
If you have chosen the Enterprise edition, you will be prompted to select the DBMS:

- **DB - Oracle Enterprise**
- **DB - PostgreSQL**

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

Press **Enter**.

3.1.3 Selecting the Installation Mode

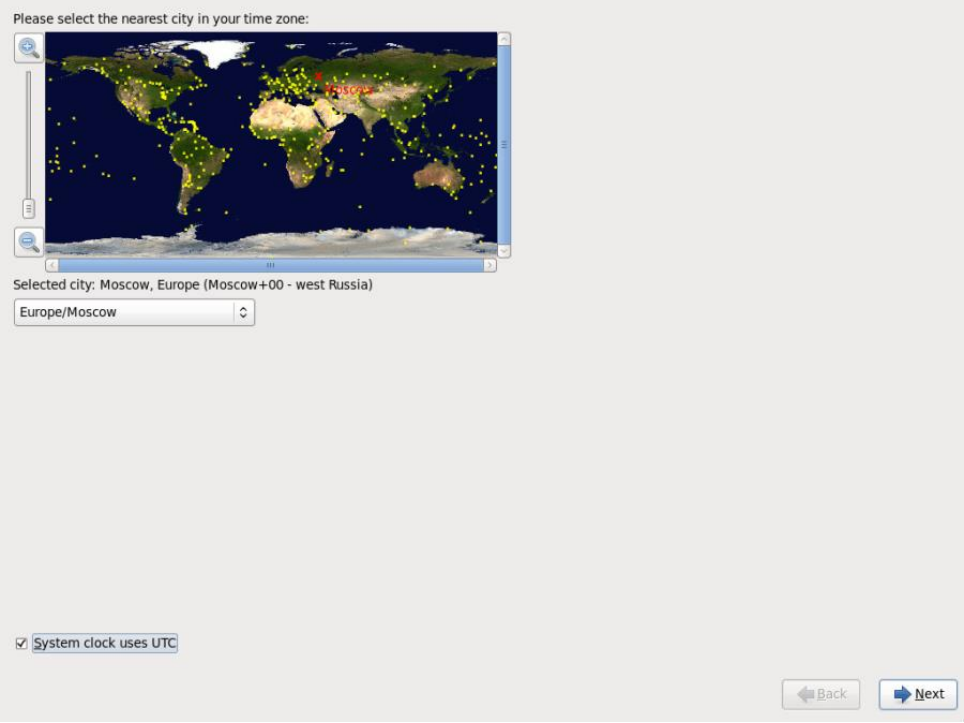


When you have selected the DBMS, you will be prompted to select the installation mode. The set of modes depends on what you selected at the previous steps. The can be the following modes:

- **TME 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 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 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.

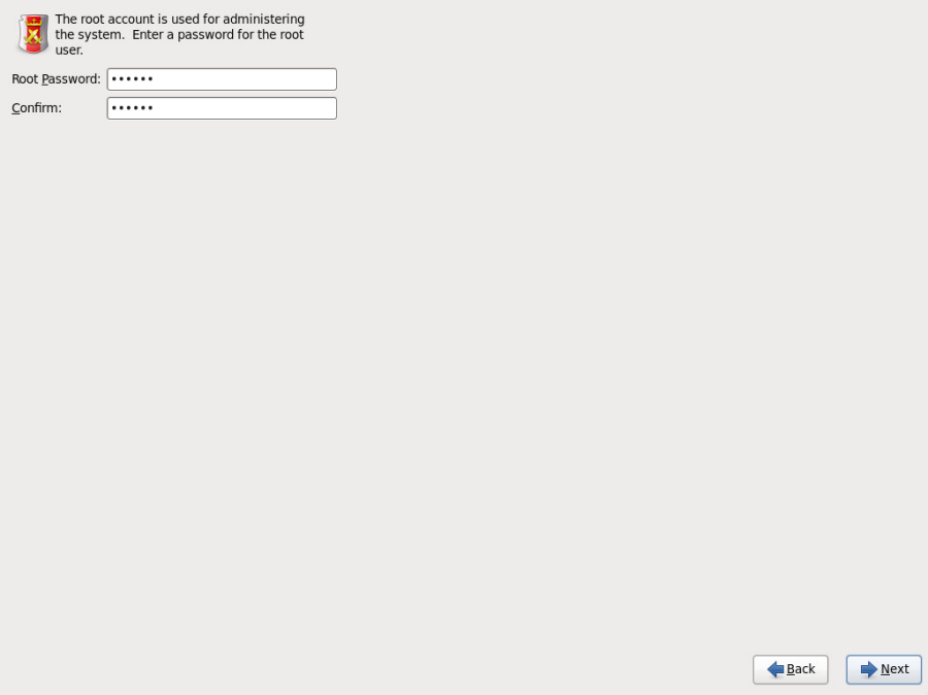
You can find your city:

- 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:

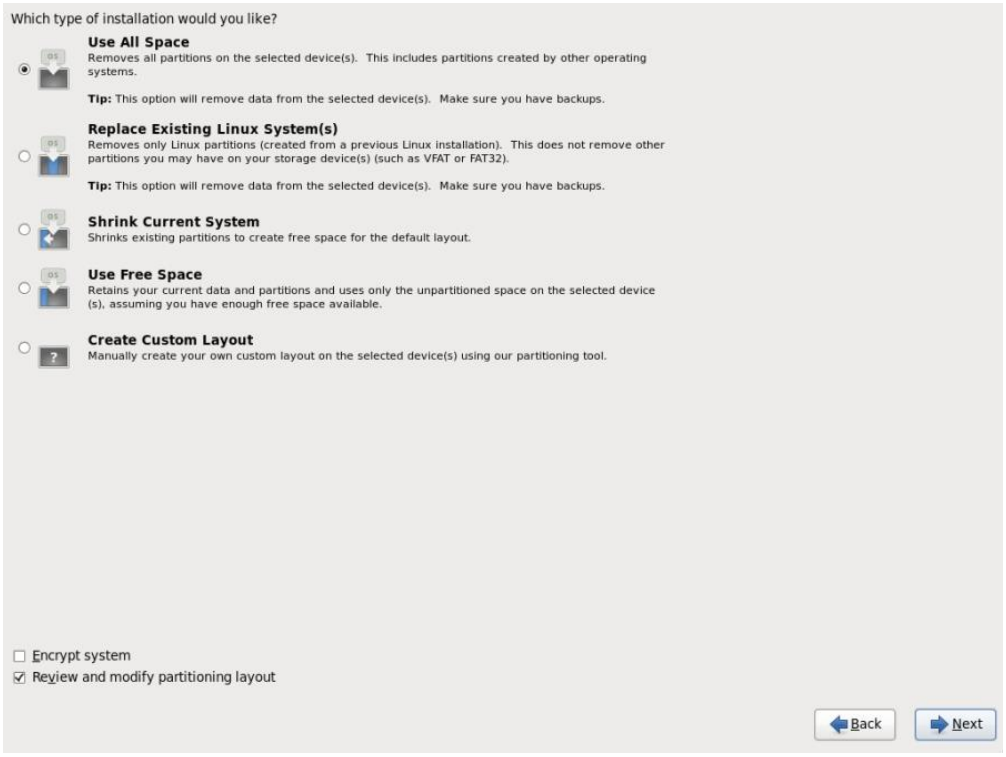
- **Use anyway** – if you want to use an entered password despite recommendations;
- **Cancel** – if you want to change the entered password.

> **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`).



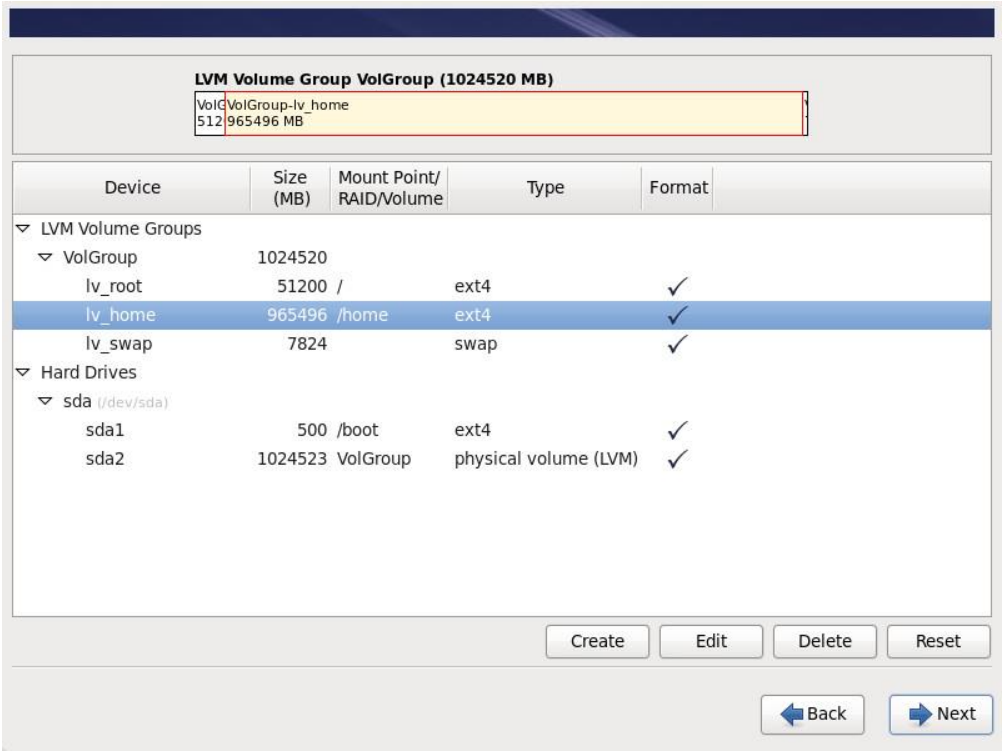
We recommend re-splitting the disc space in the following ratio:

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

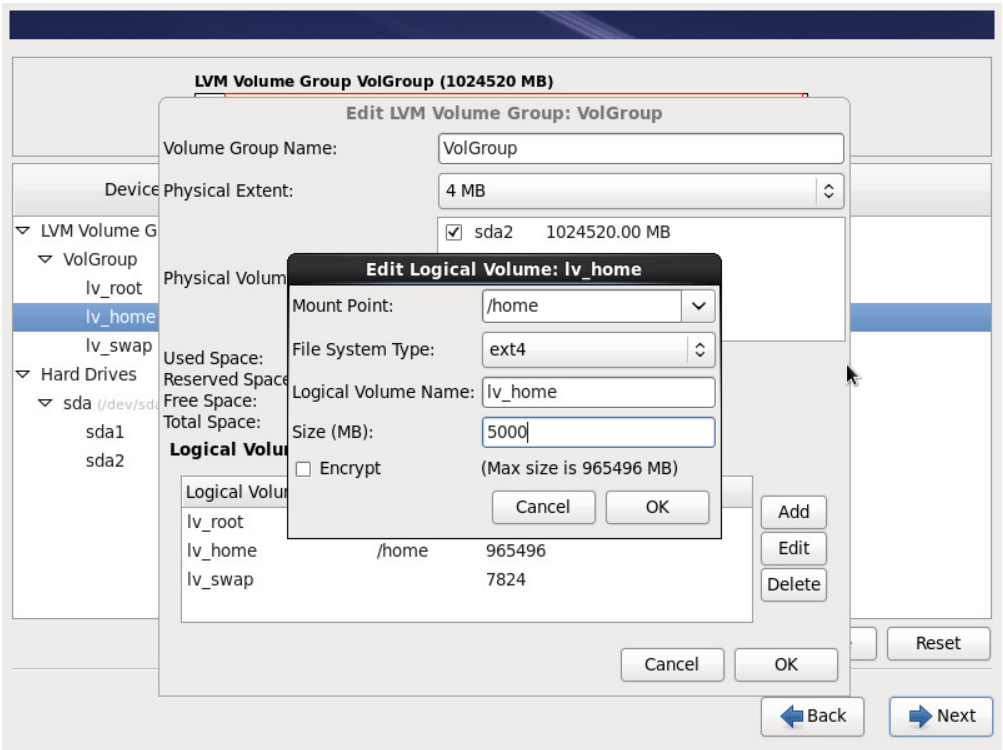
To perform this partitioning:

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**.

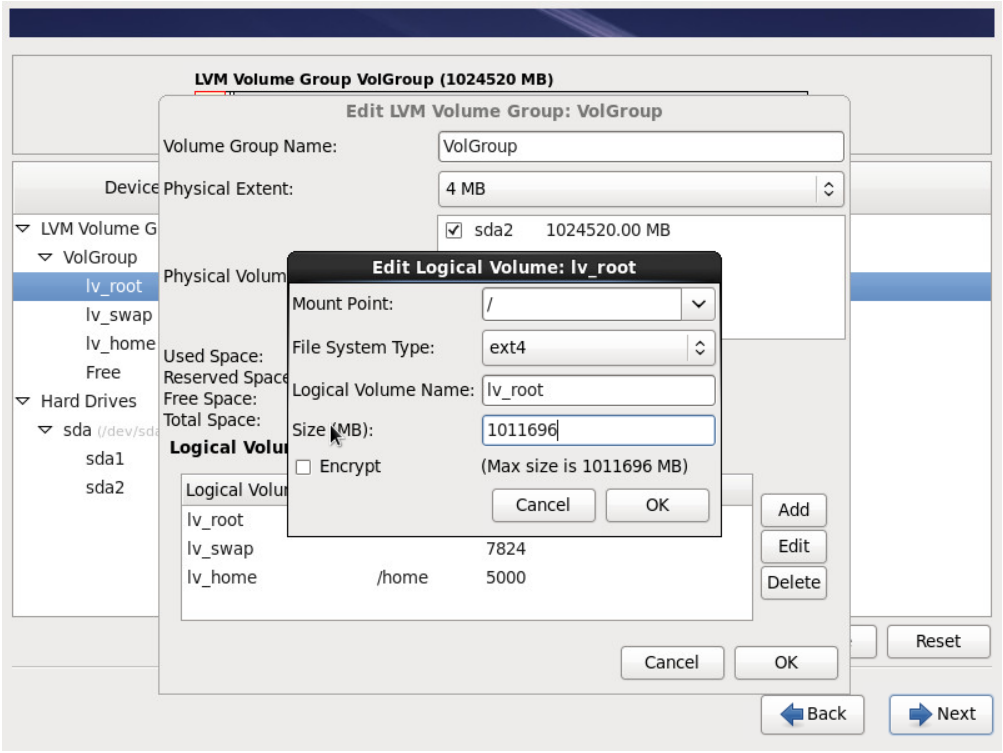
26



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**.

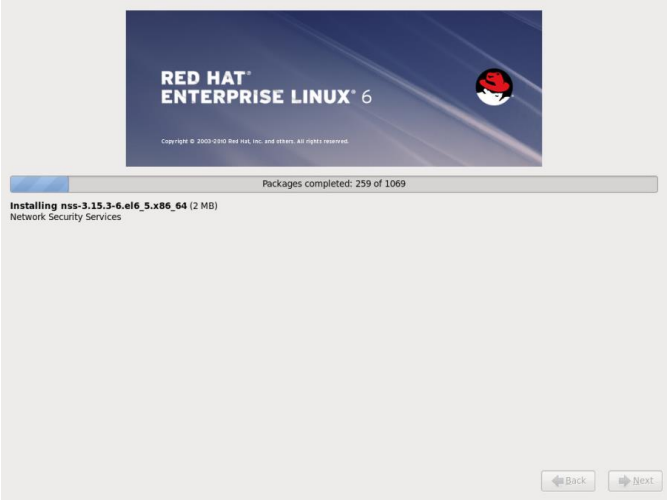


8. In **Please Select A Device** window click **Next**.

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.

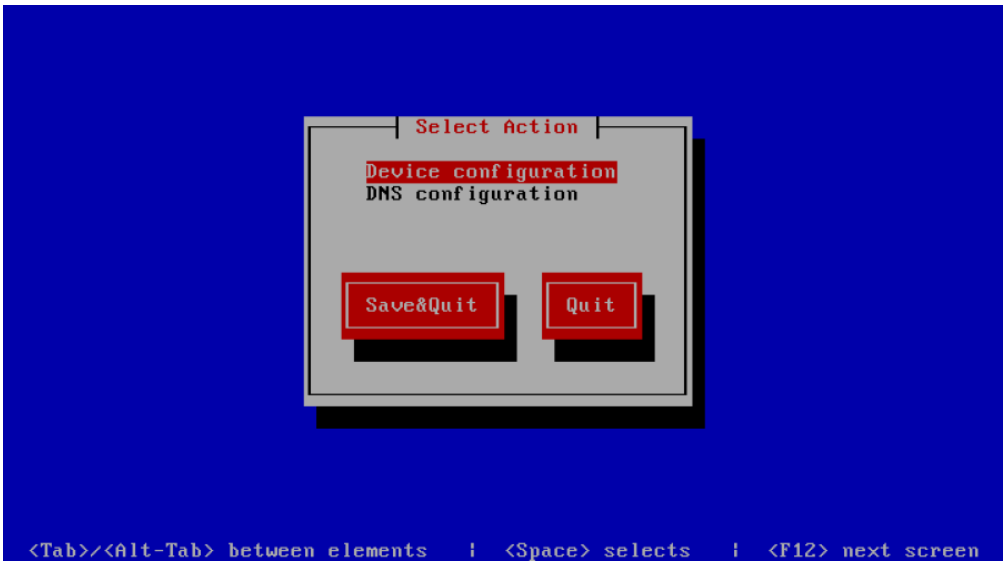
The progress will be displayed on the screen:



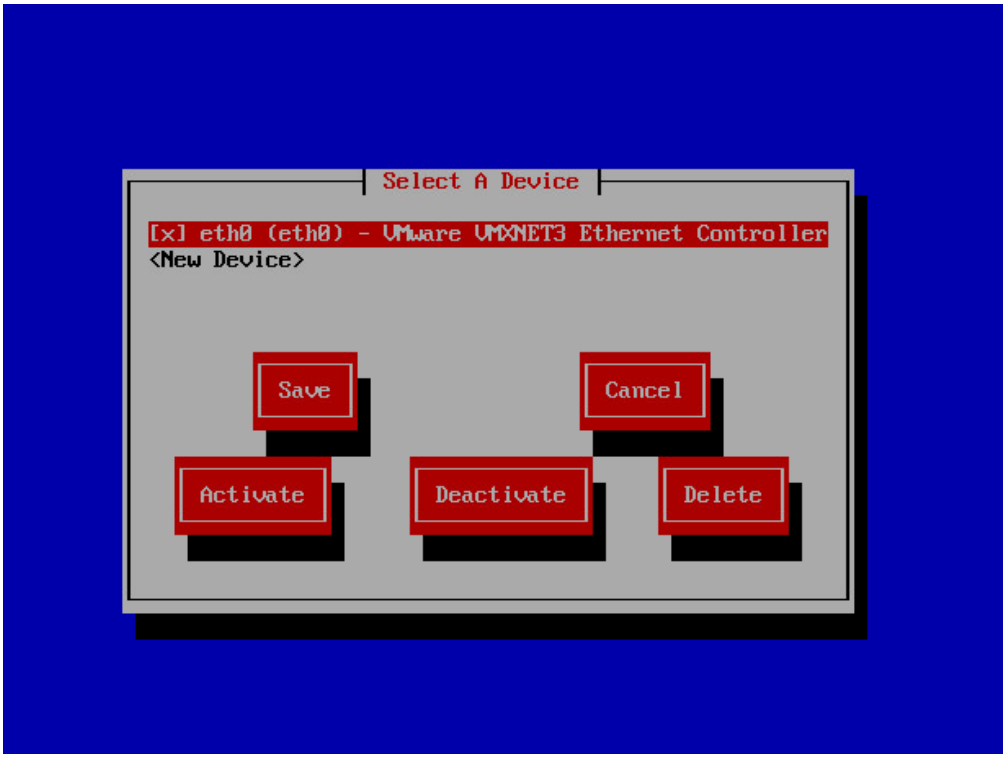
The process can take some time.

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

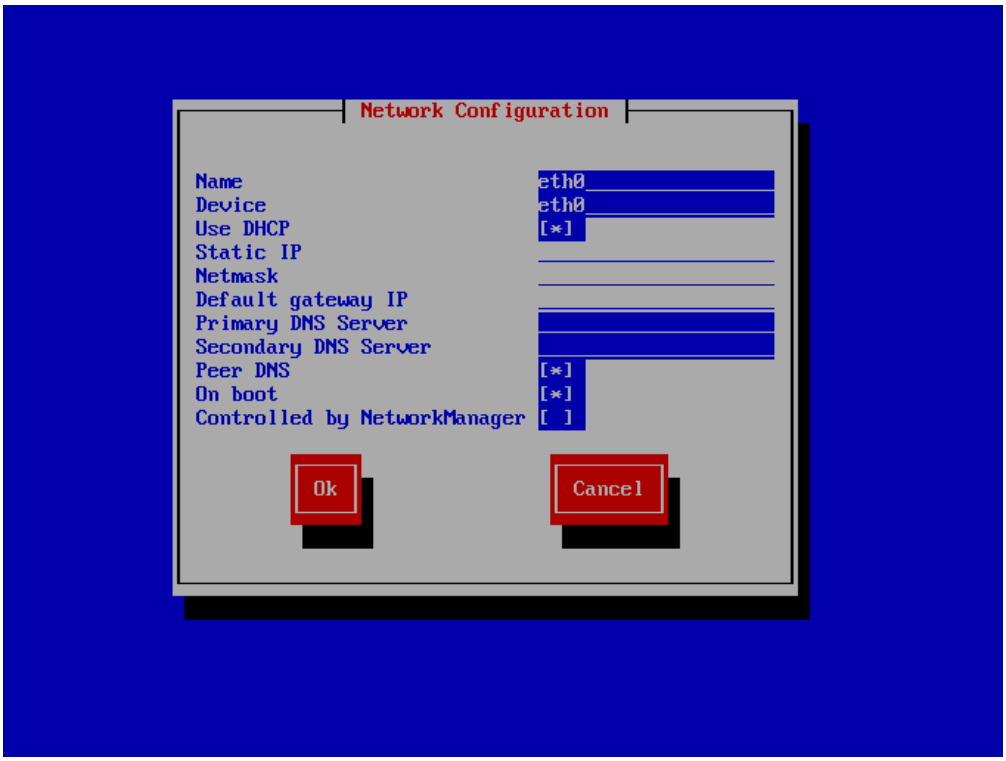


1. To set up parameters of a network card:
   a. In the **Select Action** window select **Device configuration** and press **Enter**.



   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!

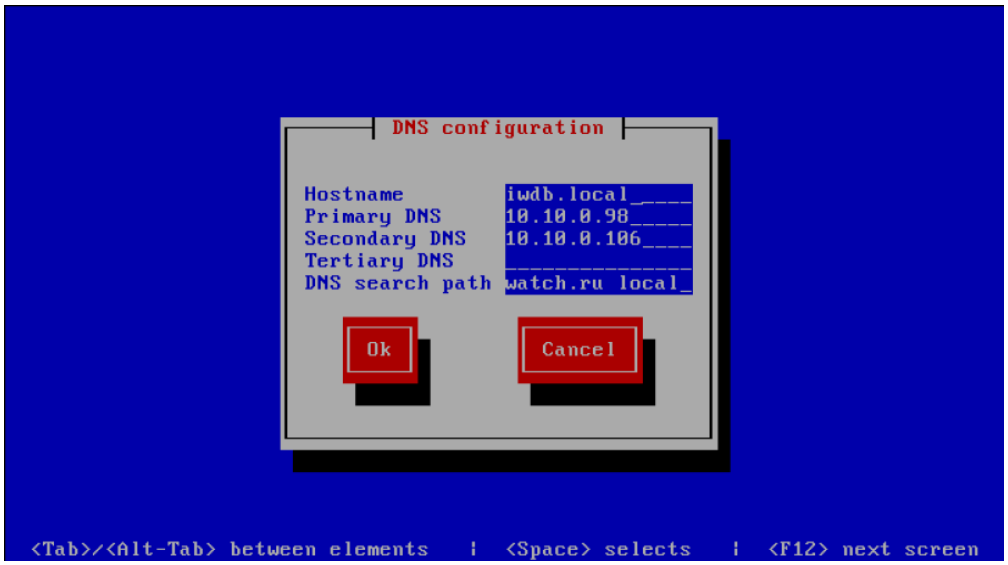
Do not use **Controlled by NetworkManager** option.

Warning!

Configuring **eth0**, make sure, that **On boot** option is enabled**.**

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

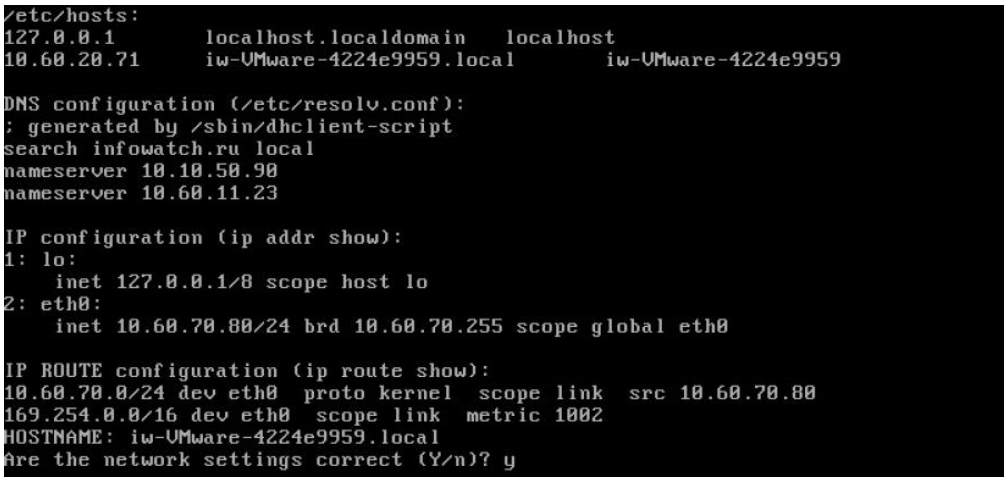
2. To configure DNS configuration in the **Select Action** window select **DNS configuration** and specify needed network settings of the server. Then click **Ok**.



Warning!

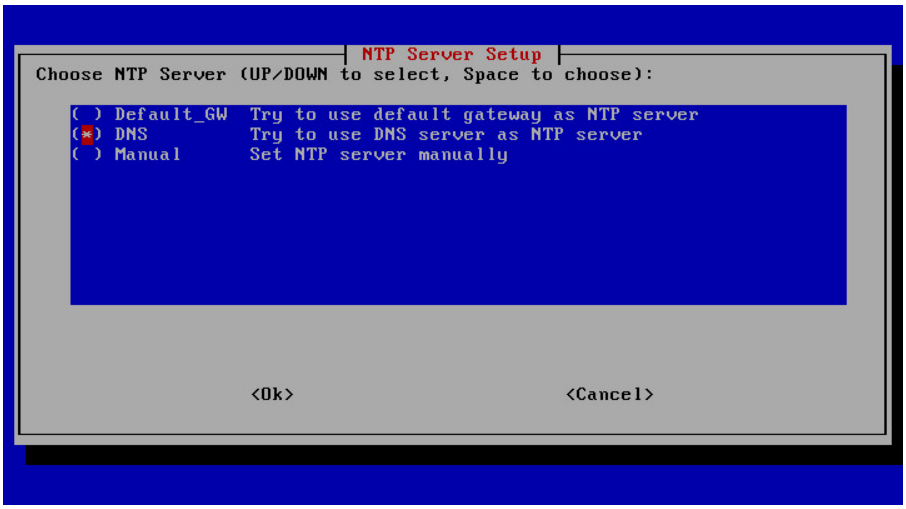
If you select **Use DHCP** in the **Network Configuration** window then instaed of parameters you specified the ones received fron DHCP will be used.

3. Click **Save&Quit**.



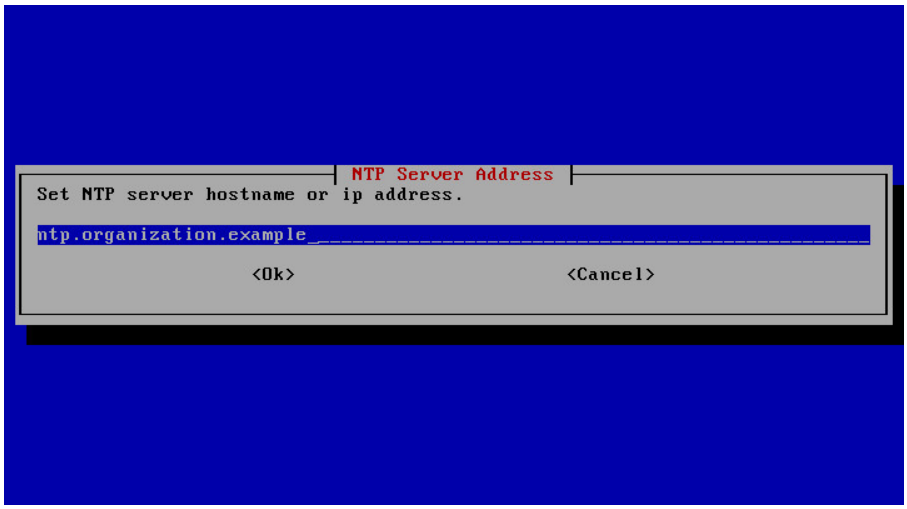
4. Examine the network settings you specified. If settings are wrong, enter **N** and specify the correct ones (see previous steps) If settings are correct, enter **Y** to confirm and press **Enter**.

3.1.8 Configuring Time Synchronization (NTP-server)



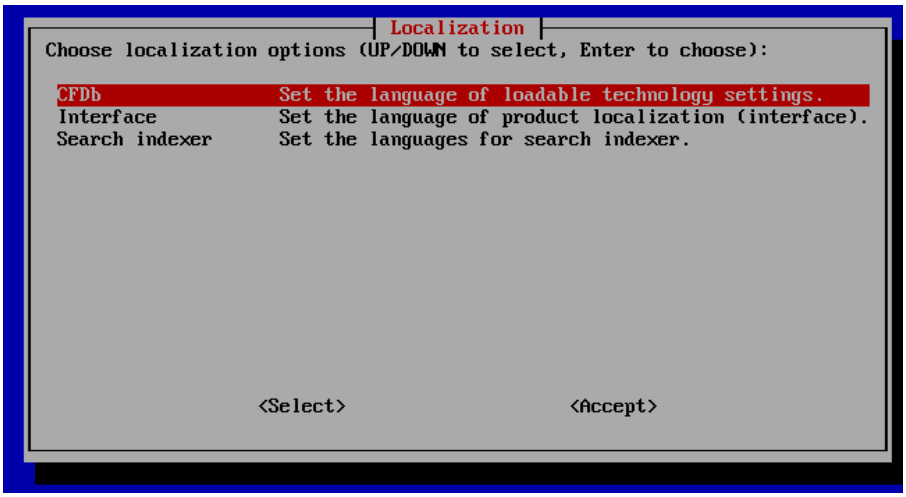
You can select one of three server setup options for time synchronization (NTP-server). Set asterisk symbol (*) in the required field and press space then click **OK**.

- **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.



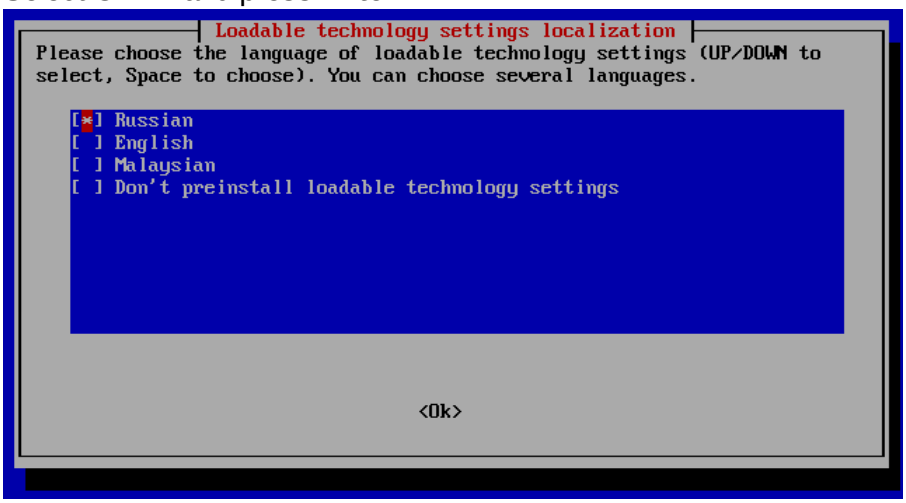
If NTP server cannot be specified for some reasons, click **Cancel** and set this parameter later; details on configuring the NTP server see in «*InfoWatch Traffic Monitor. Administration Guide*».

3.1.9 Localization Setting



To specify System localization parameters:

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



   There are three languages available::

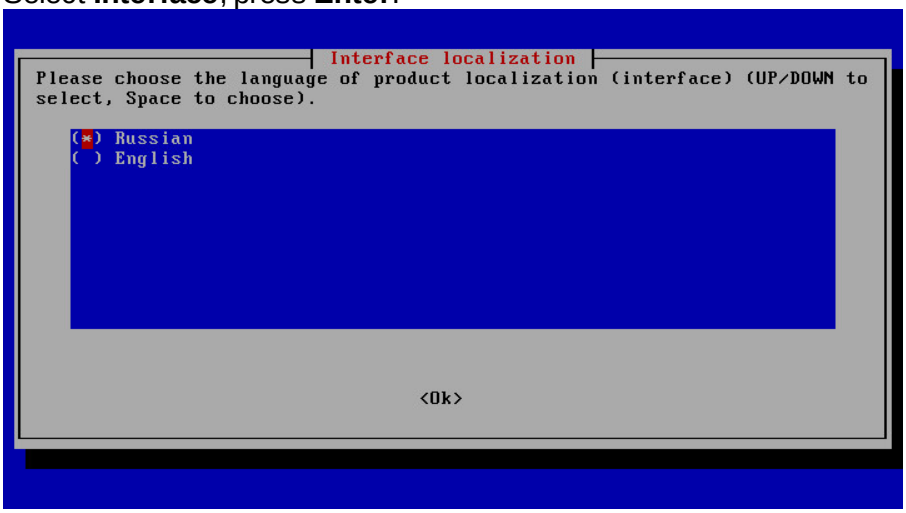
   - *Russian* – to install the Classifier in Russian;
   - *English* – to install the Classifier in English;
   - *Malaysian* – to install the classifier in Malaysian.

   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.
   Don't preinstall loadable technology settings option selection will allow you to install the System without it's standard configuration.

   b. Press **OK**.

2. Specify language for Management Console:

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

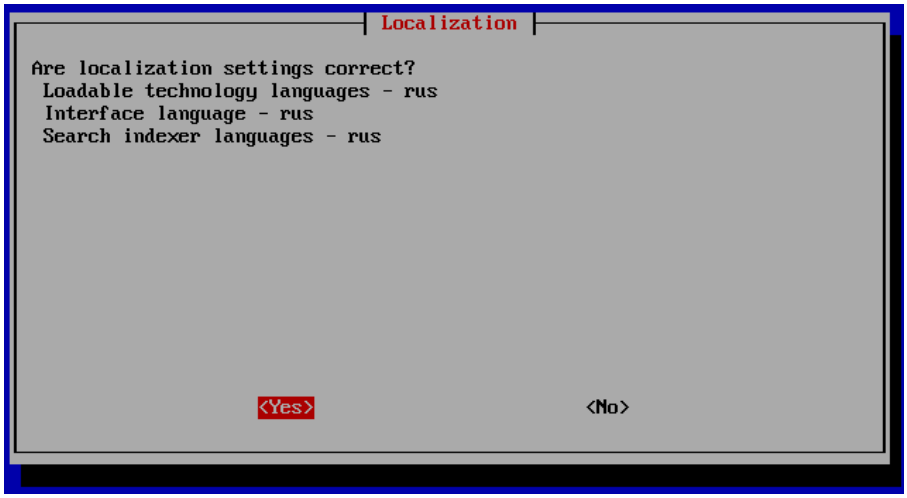


There are two languages available:

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

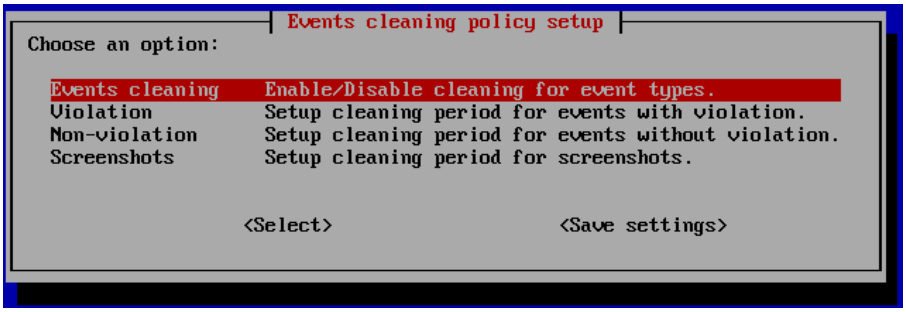
b. select required interface language and press **OK**.

3. Choose language for Search indexer:
   a. Select **Search indexer** and press **Enter**.
   b. Specify one or several languages.
   c. Press **OK**.
4. After selecting localization parameters, press **Accept**.



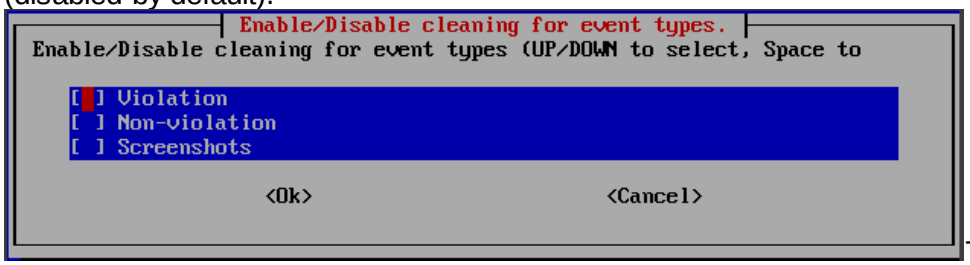
5. In the opened window check, whether parameters have been specified correctly, press **Yes**.

3.1.10 Configuring the Automatic Event Deletion from the Database



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

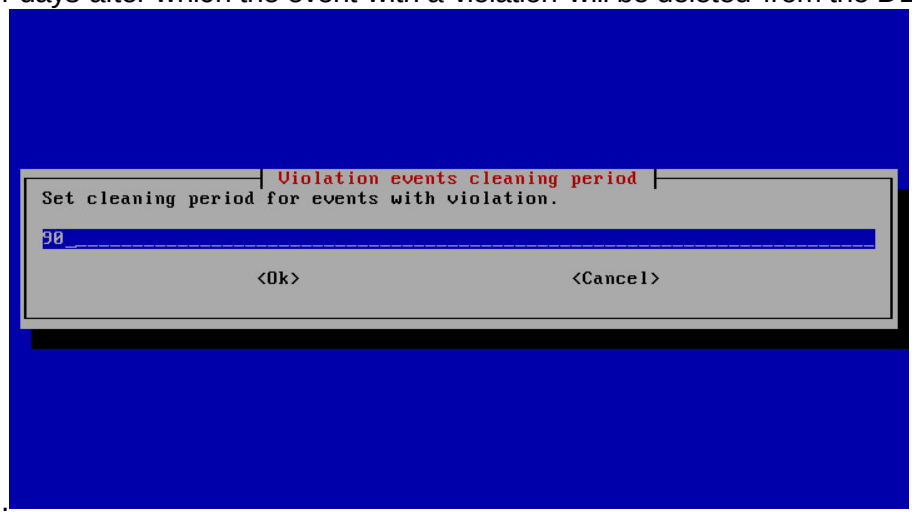
- **Events cleaning** – configures enabling and disabling of the automatic deletion of two event types (disabled by default).



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

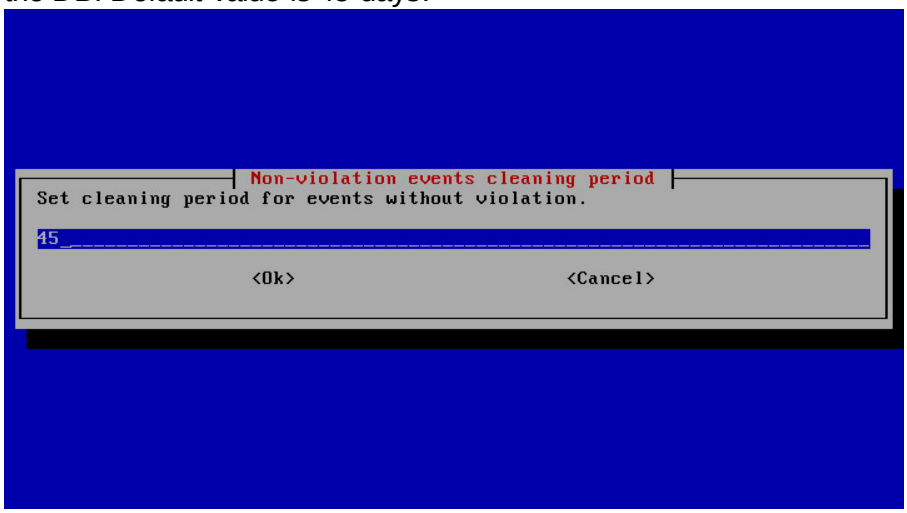
  - **Violation** – enables automatic deletion of events which violate the security policy (see details on policies in "*InfoWatch Traffic Monitor. User Guide*")
  - **Non-violation** – enables automatic deletion of events which do not violate the security policy of the company
  - **Screenshots** –enables automatic deletion of screenshots received from Device Monitor Clients.
    If necessary, you can select several items.
    Click **Ok**.

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



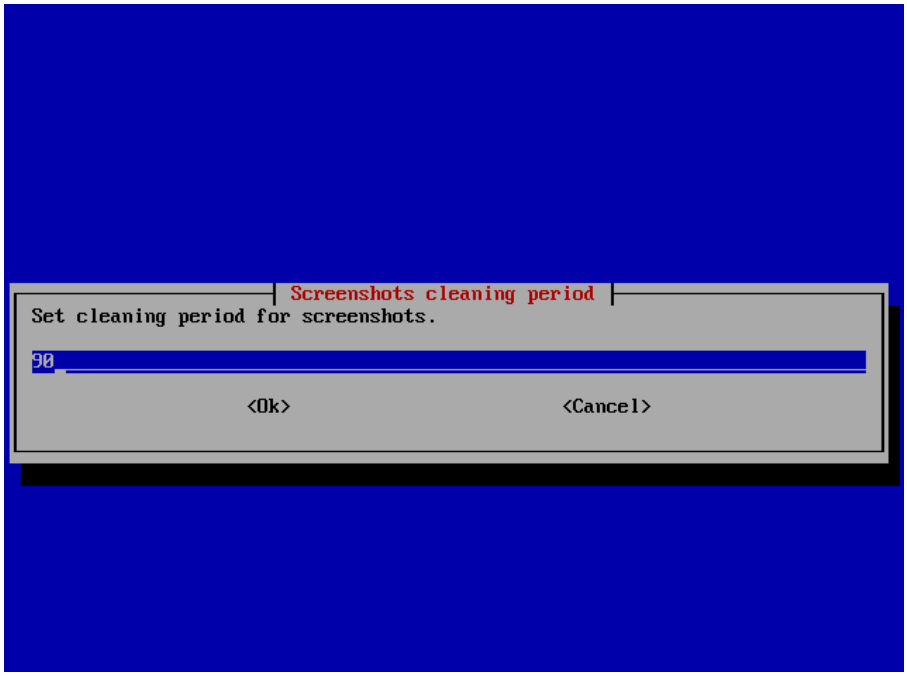
The default value is 90 days.
Enter the period of deletion, in days. Click **Ok**.

- **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**.

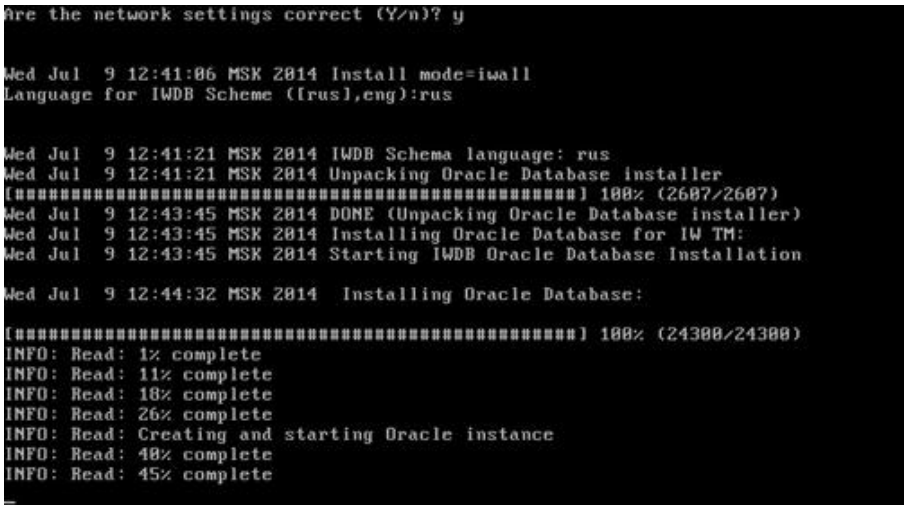
- **Screenshots** – sets a number of days after which screenshots, received from DM Client will be deleted.



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.

> **Important!**
>
> When you install **TM Standard** edition, you can select only PostgreSQL database.

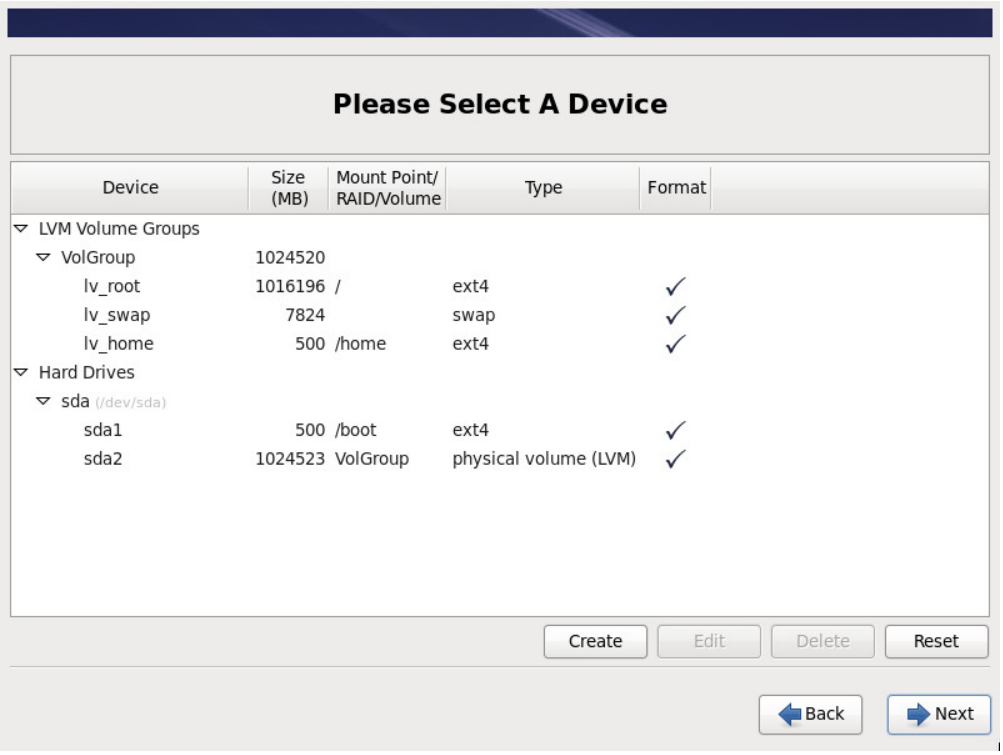
Then press **Enter**.

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**.

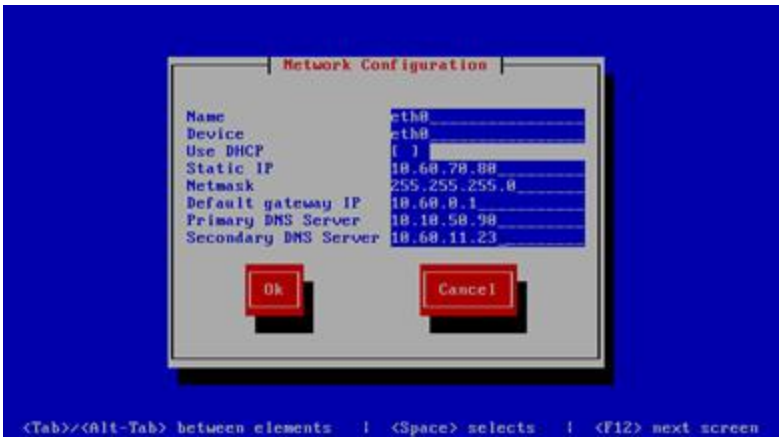


h. Click **Next**.

> **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**.

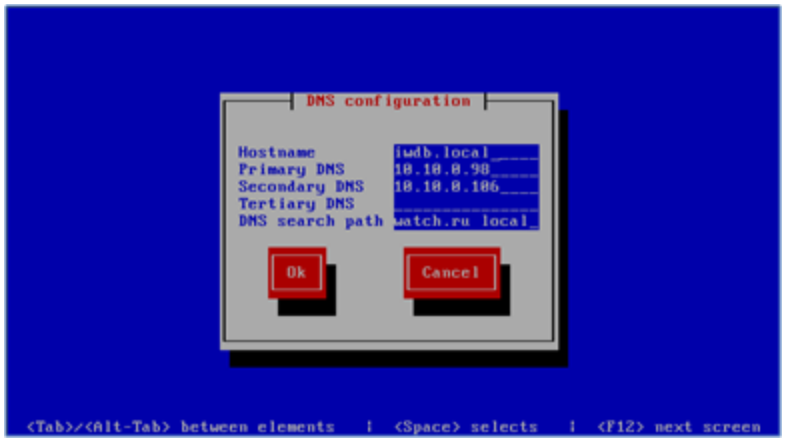


c. If you want network settings of DHCP server to be used in the System, move the cursor to the **Use DHCP** field and press Space. Otherwise, specify network settings for the server manually (static IP-address of the computer, etc.). Upon completion, click **OK**.

> **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.
        iii. If you select **Don't preinstall loadable technology settings** option, the standard System configuration is not installed.
        iv. 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.
        The Management console will be installed in selected language.
        iii. Click **OK**.
    c. Set the language of the search indexer:
        i. Select **Search indexer** and press **Enter**.
        ii. Select one or more languages.
        iii. Click **OK**.
    d. Click **Accept**.
    e. 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.
  - **Screenshots** – enables automatic deletion of screenshots received from Device Monitor Clients.
    If necessary, you can select several items.

  Click **Ok**.
- **Violation** – sets a number of days after which the event with violations will be deleted from the DB (by 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 (by default: 45 days).
  Enter the period of deletion, in days. Click **Ok**.
- **Screenshots** – sets a number of days after which screenshots received from Device Monitor Clients will be deleted from the DB (by default: 90 дней).

  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.

3.3.1 Installing Database (TM DB Server)

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. In the Welcome window select **TM Enterprise** and press **Enter**.
2. In the database selection window specify which DBMS should be installed:
   a. Oracle Standard;
   b. PostgreSQL.

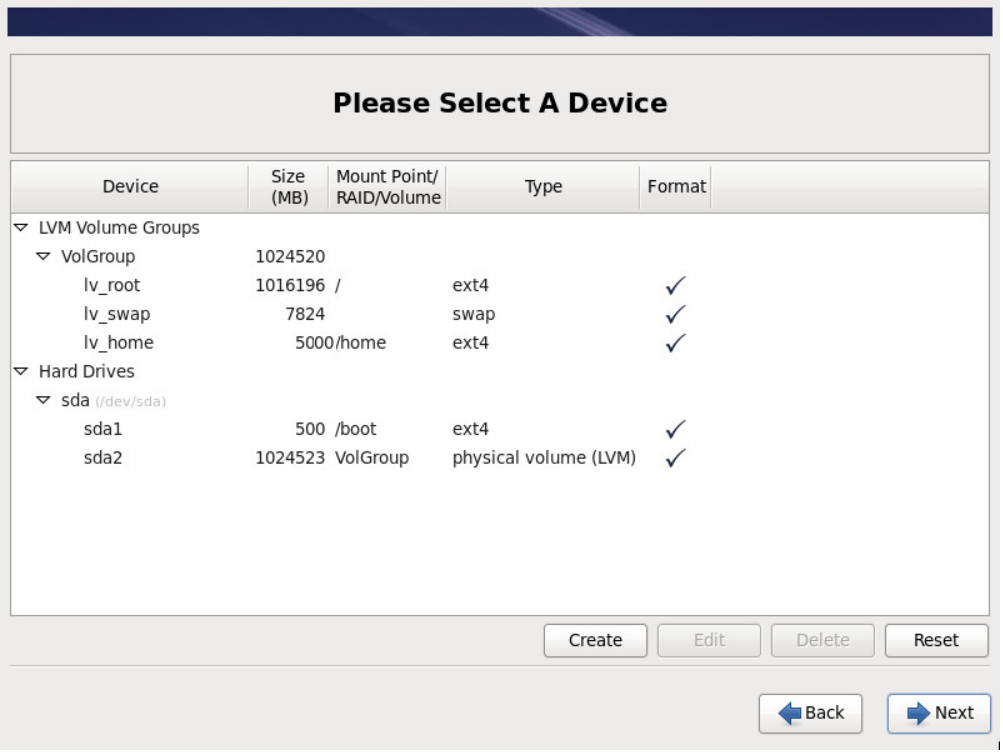
   Click **Enter**.
3. In the window of selecting the installation mode, choose **TME DB server** and press **Enter**.

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.

4. 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**.
5. Specify a password for *root* superuser and click **Next**. Recommendations on password creation are available in Appendix A

6. 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.

7. Configure parameters of a network card and DNS as described in "Network Settings". Click **Save&Quit**.
8. 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**.
9. Specify server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field and press **Space**, then click **OK**.

10. 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. Set language for Search indexer:
        i. Select **Search indexer** and press **Enter**.
        ii. Specify one or several languages.
        iii. Press **OK**.
    d. Click **Accept**.
    e. In the opened window make sure the selected languages for pre-installed settings and interface are specified correctly, then click **Yes**.
11. 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**.
    - **Screenshots** – sets a number of days after which screenshots, recieved from DM Client will be deleted from the DB (default: 90 days).
12. 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.

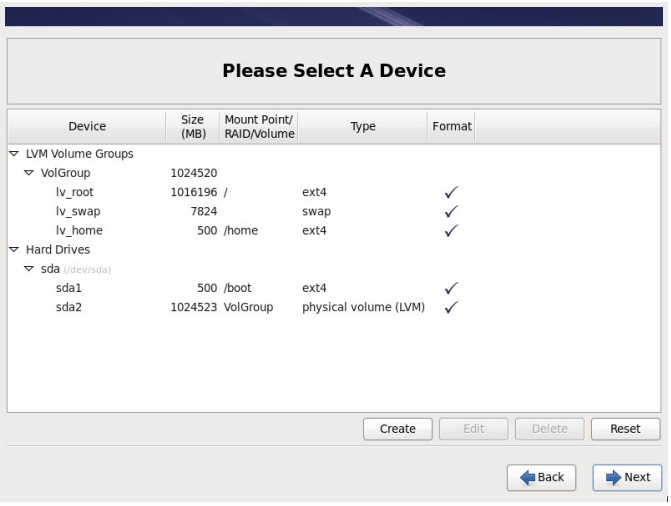
c. Click **Next**.

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 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.

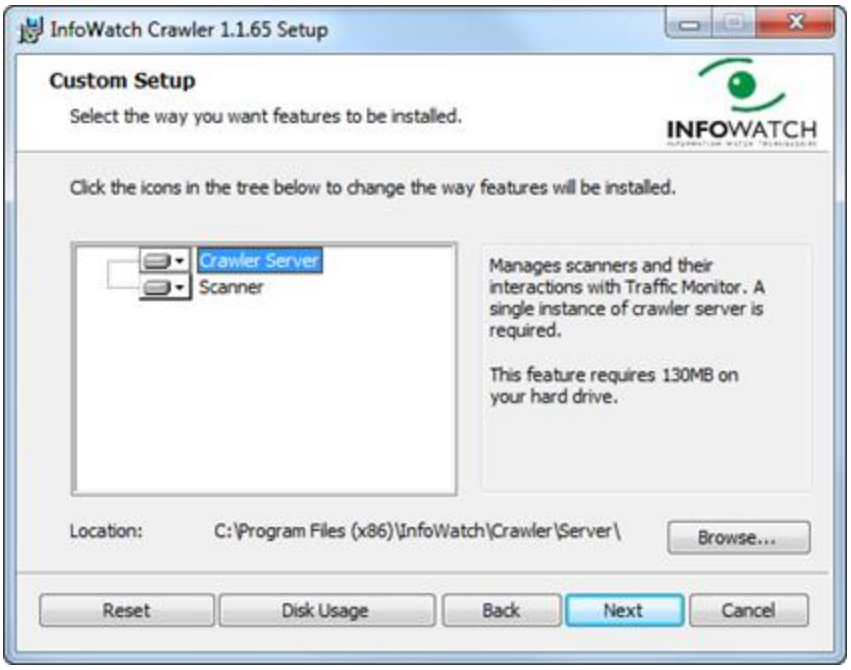
To install Crawler:

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

Note:

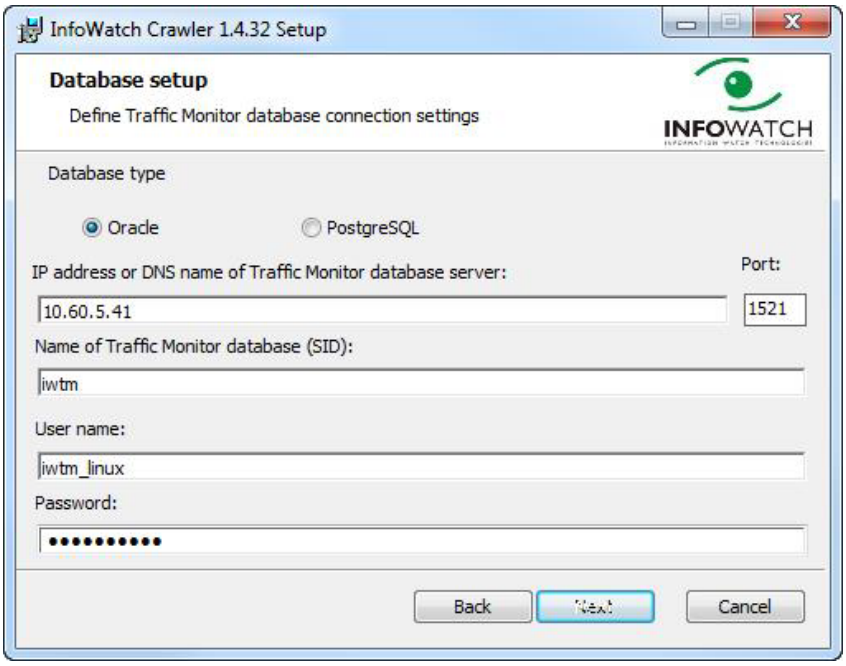
The language of the Installation Wizard is defined automatically and depends on the selected format (see **Start -> Control Panel -> Region and Language**, **Formats** tab).

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**.

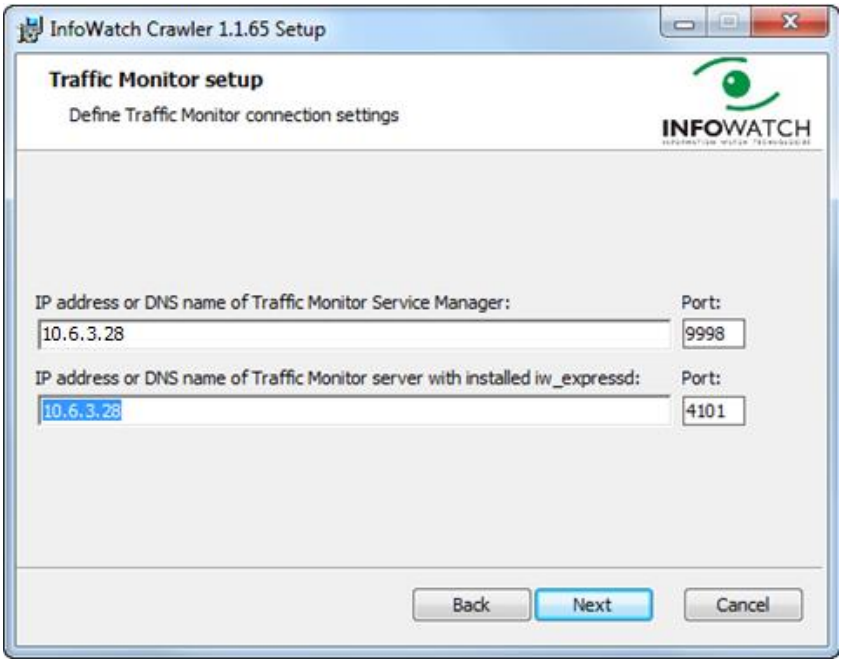
5. If at the **Custom Setup** step, you have chosen the **Server Crawler**:
   a. Specify parameters for connection of the `InfoWatch.Crawler.Server` service with Traffic Monitor database, click **Next**.



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.

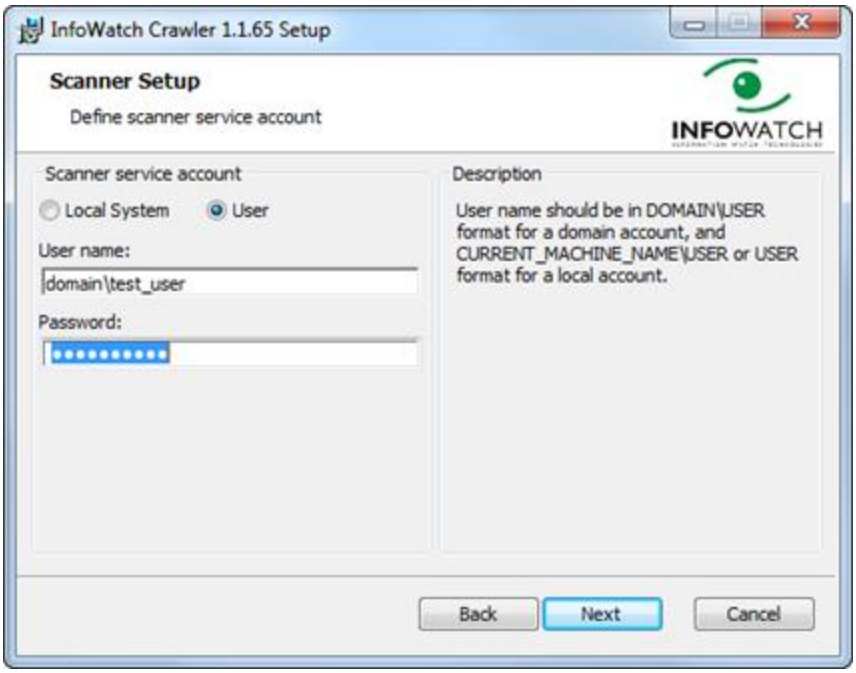
b. Specify parameters for connection of the `InfoWatch.Crawler.Server` service with Traffic Monitor server, click **Next**.



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`.

3.5 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

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 **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**

3.6 Installing InfoWatch Device Monitor

Installation is performed in the following order:

1. InfoWatch Device Monitor Server End Setup.
   Server end consists of the following elements:
   - Database
   - Device Monitor Server
   - Device Monitor Management Console.
2. Installing InfoWatch Device Monitor Client End.
   Client is installed on each computer that should be controlled by InfoWatch Device Monitor.

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

3.6.1 InfoWatch Device Monitor Server End Setup

InfoWatch Device Monitor server end is installed with universal Setup Wizard.
Universal Setup Wizard disk is available on your System installation CD (Setup.Unified directory). This program lets you install all System components except the Client: database, Device Monitor Server, and Management Console.
The InfoWatch Device Monitor system can use Microsoft SQL Server or Oracle DBMS or PostgreSQL for managing the database.
Management Console connects to the primary server.
For more information on installation, see:

- Database deployment under Microsoft SQL Server DBMS
- Database deployment under Oracle DBMS
- InfoWatch Device Monitor Server Setup
- InfoWatch Device Monitor Server End Installation Procedure

3.6.1.1 Database deployment under Microsoft SQL Server DBMS

You must install Microsoft .NET Framework 2.0 Service Pack 1 and Microsoft .NET Framework 4.0 or higher before launching database scheme generation on your computer.

Database generation account must be configured in advance. Account type depends on database server authentication. Microsoft SQL Server DBMS supports two types of authentication:

- **Windows authentication**. Authentication uses accounts within Windows domain. Authentication data is processed by Microsoft Windows security.
- **SQL Server built-in authentication**. Uses Microsoft SQL Server accounts. Authentication is carried out via DBMS.

Important!

To ensure satisfactory safety level, we strongly recommend that you use **Windows authentication** method.

If you are going to use Windows authentication method:

1. Make sure Windows domain contains only one account that you will use for database generation. This account must have local administrator privileges on the computer used for database generation. If necessary, create a new account.
2. Add the account to Microsoft SQL Server DBMS and select **Windows authentication**.
3. Assign **dbcreator** role to the account.

If you plan to use SQL Server built-in authentication method:

1. Create a new Microsoft SQL Server account. When configuring an account: select **SQL Server built-in**, enter user name and password.

2. Assign **dbcreator** role to the account.

> **Note:**
>
> Integrated account name and password are specified when configuring the database (see "InfoWatch Device Monitor Server End Installation Procedure", step 6).

3.6.1.2 Database deployment under Oracle DBMS

The following components should be installed on the computer before launching the database schema generation:

- Oracle DBMS client
- Oracle Database Provider for .NET (ODP.NET)

> **Important!**
>
> Enable this feature by selecting the corresponding field in the Custom installation type. Installation must be run under the administrator account.

Before you start creating a database scheme, make sure that **tnsnames.ora** file contains database server connection parameters (see "Configuring ORACLE DBMS connection").

3.6.1.2.1 Configuring InfoWatch Device Monitor connection to Oracle DBMS server

To ensure proper connection to Oracle DBMS server for each computer with Oracle DBMS client, you must configure `tnsnames.ora` file located in `[ORACLE_HOME]\network\admin` directory.

Configuring tnsnames.ora

Specify Oracle DBMS server connection settings. To do this, add the following entry to `tnsnames.ora` file:

```
tns_name =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = service_name)
)
)
```

Specify true values for the following parameters:

- `tns_name` – Oracle DBMS server alias;
- `host_name` – Oracle DBMS domain name or IP address;
- `port_number` – server port for listening to client connections;
- `service_name` – database service name.

Example of `tnsnames.ora` file:

```
IWDM =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

Important!

The `tnsnames.ora` file is format sensitive. If you copy an example to edit a file, make sure that the copied selection does not contain any blank strings.

3.6.1.3 Server Setup Recommendations

To enhance the performance of Device Monitor, we recommend that you should deploy the server and database on separate computers.

Important!

When deploying a multiple-server pool, each server must have the same InfoWatch Device Monitor server application version installed that is compatible with the appropriate up-to-date database.

To make the InfoWatch Device Monitor Server able to install the Clients onto mobile devices, the server should have a long name. If the used server is not in the Windows domain then you need to configure FQDN. To do this:

1. In the **System Properties**, on the **Computer Name** tab click **Change**.
2. In the **Computer Name/Domain Changes** dialog window, click **More**.
3. In the **Change primary DNS suffix when domain membership changes** field, enter the domain name.
4. Click **OK**.
5. Make sure that the **Full computer name** field displays the long name.

While configuring the Server (see "InfoWatch Device Monitor Server End Installation Procedure"), you must specify the account that will be launching InfoWatch Device Monitor Server. Available options:

- **Local System**. Launch service from system account.
- **User**. Launch service from Windows domain account.

For Microsoft SQL Server DBMS database. If you select **Windows authentification** for database owner (see "Database deployment under Microsoft SQL Server DBMS"), while database and Server are on separate computers, select **User** variant.

Important!

It is not recommended to select Local System option. In this case, the user can obtain unlimited rights, which contradicts the security policy.

Windows domain account (**User**) must be configured in advance. To do this:

1. Allow the account to run process as a service:
   - In the **Control Panel** open **Administration** > **Local security policy**.
   - In the following dialog select **Local policies** > **Assign User Rights**.
   - Double-click **Log on as service** in the right **Details** pane.
   - On **Local security parameter** tab add the account.
2. Add a new account to Microsoft SQL Server DBMS account list.

When setup finishes, allow the account to create new databases. When specifying database access permission, select **db_owner** role.

3.6.1.4 Server End Installation Procedure

Important!

Before starting the installation, see "Server Setup Recommendations".

Important!

When deploying a multiple-server pool, each of them must have the same InfoWatch Device Monitor server application version installed compliant with the appropriate up-to-date database.

1. **Running the Installation Wizard**

   Insert the installation CD into your CD-ROM drive. Then open `Server` directory. Run platform-specific setup file from this directory.
   You will be redirected to InfoWatch Device Monitor Setup Wizard welcome screen. Click **Next**.

2. **Accepting the License Agreement**

   Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms in the License Agreement** and click **Next.**

3. **Selecting components to install**

   Custom Setup page has all components selected by default:
   - Server
   - Management Console

- MSM module (Taiga) - component enabling Device Monitor Client installation to mobile devices (see details in "*InfoWatch Traffic Monitor. User Guide*", "Mobile Devices" section). Can be installed and used only together with the Management Console.

You can change the list of components you want to install. For example, if you want to use an existing Management Console with a new Server, you do not need to install this feature: click **Management Console** and select ✕ **Entire feature will be unavailable**.
You can also change the folder to install the component: select this component in the list, click **Browse** and specify the needed location.
Click **Next**.

4. **Configuring server settings**

On **Type of installed server** page select:

- **Primary Server** - should be installed first. Clients and Management Console will connect to it.
- **Secondary Server** - an additional server that balances Clients workload.

To ensure rapid server status updates it is recommended that you select **Publish Server in Active Directory** option.

Important!

Workstations occasionally interact with Device Monitor server to update security policies. To let the newly added server handle workstations and notify the Clients about any possible server port changes it is recommended that you publish its details in domain during the installation. To publish Device Monitordataindomain, the account that installs the server needs privileges to create and delete connection points.

If you have the Device Monitor database of the appropriate version, deselect **Install new Database** option.
Click **Next**.

5. **Choosing configuration file**

If the installation of the new database is not performed, this step is skipped.
To use the server configuration file exported before (see "*InfoWatch Traffic Monitor. User Guide*", "Import/Export Configuration" article), click **Open** and specify configuration file location.

Important!

The configuration file should be placed on the local hard or external device. The Setup Wizard does not support network locations.

Click **Next**.

6. **Selecting database server**

Specify DBMS that will control Device Monitor database by choosing one of the following options:

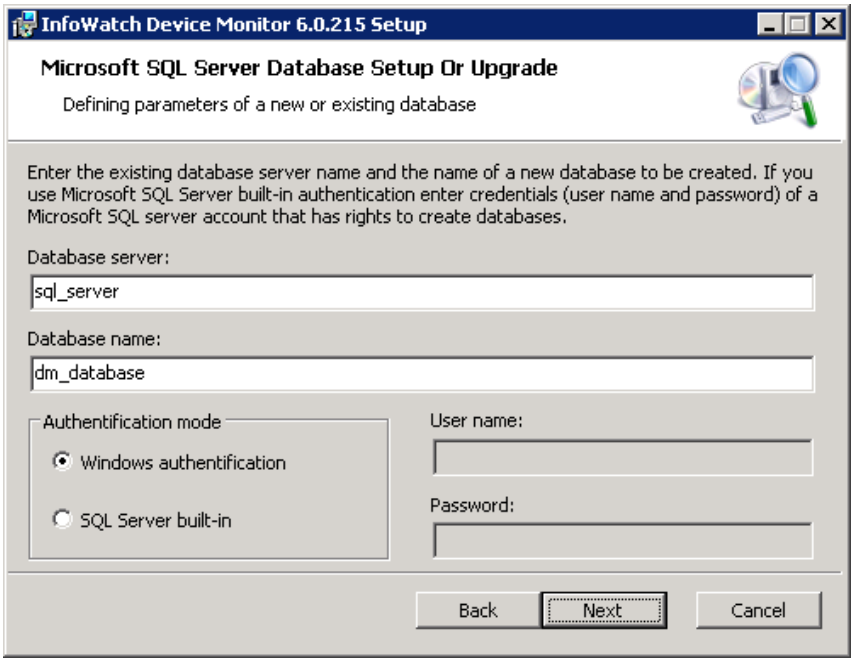
- Microsoft SQL Server
- Oracle
- PostgreSQL

If you don't want to install a new database (**Install new Database** option has not been selected in Step 4), you need to specify connectivity settings for existing Device Monitor database.
Click **Next**.

7. **Database configuration**

You skip this step if you chose to use an existing database in Step 4.
Database configuration depends on DBMS type.
If you are using Microsoft SQL Server DBMS, specify the following parameters:

- **Database server**. NetBIOS Microsoft SQL Server name where the database will be created. Do not enter IP address in **DB server** box, since this will prevent you from connecting to the database server.
  If there are any named instances on the database server, specify server name as follows: <server_name>\<instance_name>.
- **Database name**. New database name.
  It may contain Latin letters, numbers, and other characters except spaces and special characters: «*», «?», «/», «\», «|», «^», «:», «"". Name must start with a Latin letter.
  Name may be 1 to 123 characters long.
- **Authentication mode**. Database owner authentication method. For this option, specify the authentication method selected during account preparation (see "Database deployment under Microsoft SQL Server DBMS").
  If the account uses Windows authentication, select **Windows authentification**. In this case, the database will be created by the domain user, who runs the installation.
  If the account uses SQL Server authentication, select **SQL Server built-in**. Then enter username and password into **User name** and **Password** fields respectively.



When using Oracle DBMS configure the following settings:

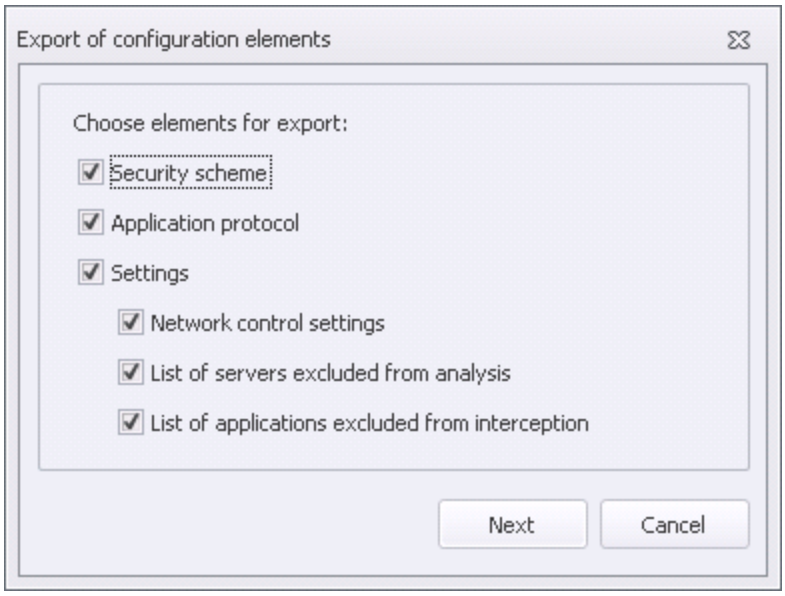
a. Set database server connection options:
- **Database server**. Database server name. Use server alias from `tnsnames.ora` file for this parameter.
- **The password of 'SYSTEM' login**. SYSTEM account password.

b. Specify the parameters of database schema owner account:

> **Important!**
>
> It is not recommended to use existing database scheme settings.

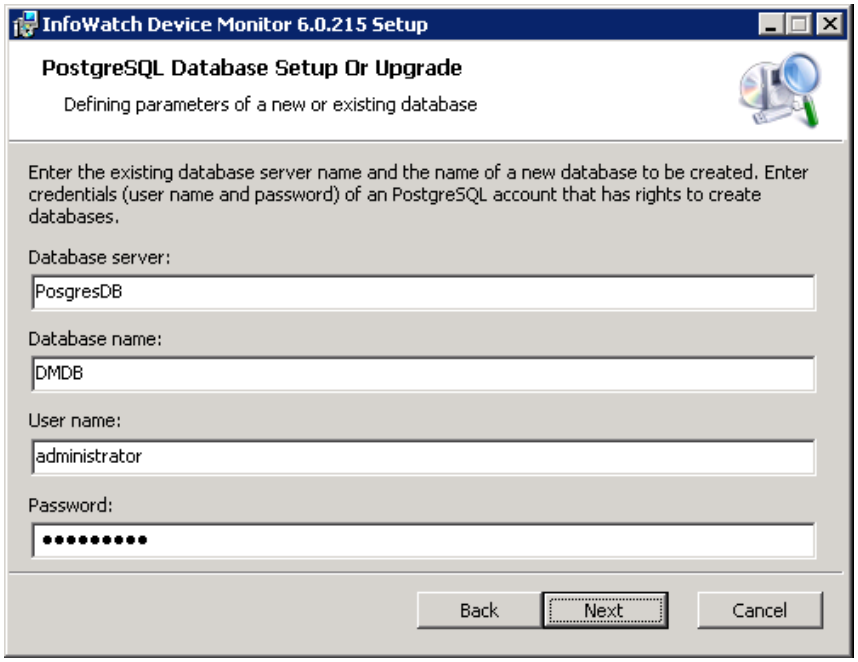
- **Scheme owner**. Database schema owner account name.
- **Password, Confirm password**. Database schema owner account password.
Password is assigned basing on requirements specified in Oracle DBMS documentation.

c. Configure tablespace settings in **Tablespace** box.
You can use existing tablespace or create a new one. If you are using existing tablespace, enter the tablespace name in **Name** field.
To create a new tablespace, check the **Create new** box. Then specify tablespace options:
- **Name**. Tablespace name.
- **File name**. Name of the file where the new tablespace will be stored.
- **Size**. Maximum size (in MB) of the data file (default size is 3000 MB).
- **Extent size**. Maximum size (in MB) of continuous segment in data file (the default size is 1 MB).
- **Autoextension**. Automatic file extension via Oracle DBMS. If Autoextension box is selected, automatic extension is enabled (this feature is disabled by default).



When using PostgreSQL configure the following settings:

- **Database server**. The name of the PostgreSQL DBMS where the database will be created.
- **Database name**. The name of the newly creating database.
  It may contain Latin letters, numbers and other symbols excluding spaces and special symbols: «*», «?», «/», «\», «|», «^», «:», «"». Name must start with a Latin letter.
  Name may be 1 to 123 characters long.
- **User name** - the name of the account having rights for creating the DB on the PostgreSQL server.
- **Password** - the password of the account having rights for creating the DB on the PostgreSQL server.



After all necessary parameters have been configured, click **Next**.

8. **Configuring the server**

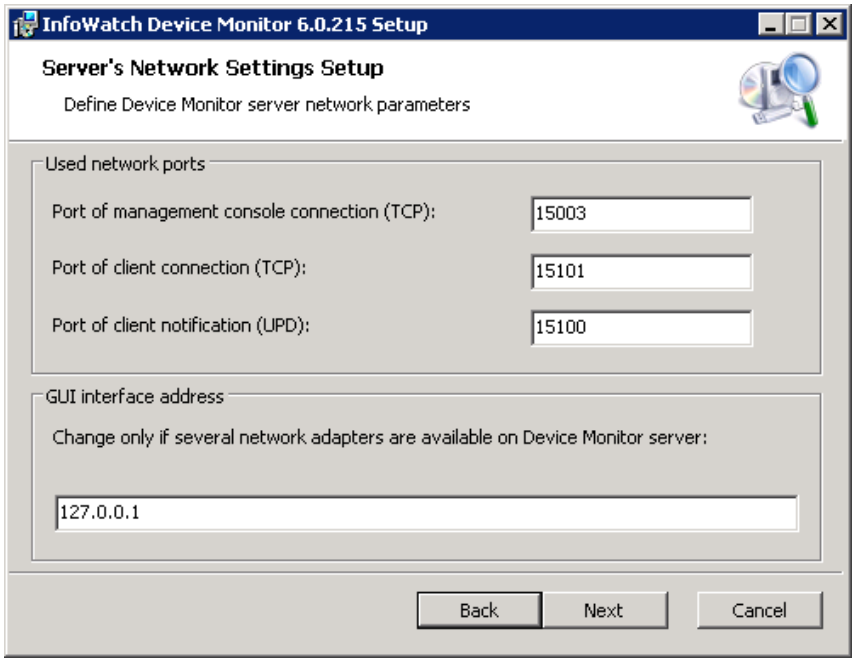
Configure Server parameters:

a. In **Used network ports** box set TCP and UDP ports used for:
- **Management Console connection**;
- **Clients connection** to transfer security schemes to managed workstations, send information about events and shadow copies to server;
- **Clients notification** about security scheme changes.

b. In **GUI interface address**, enter the IP address that will be used for interaction between Server and Management Console.

Important!

This value should only be changed if the Server is installed on a computer with multiple network adapters connected to different networks. If there is one network adapter, this value must remain unchanged, otherwise Management Console won't be able to connect to Server. If you add more network adapters while working with Server, you can change this setting in Server configuration file.



After all necessary parameters have been configured, click **Next**.

9. **Configuring secure channel**

Specify the port used for traffic transfer between the InfoWatch Device Monitor Client and Server.

If you install a new database (Install new Database option was selected in Step 4), then in Secure channel key area select:

- if you perform the first installation then leave the **Create new key** setting;
- if you used the server of version 6.0 or higher and deleted it and then you install it again, then to make Device Monitor Clients could connect and bind to the new server, you should specify the encryption key used on the old server. The recommendations on saving the encryption key are listed in "Uninstalling InfoWatch Device Monitor". Select **Use existing key** and specify the path to the file of the encryption key.

Click **Next**.
If you selected **Create new key** setting, specify the path where Device Monitor will save file with a generated key.

10. **Configuring server account**

Select an account that will launch InfoWatch Device Monitor according to "InfoWatch Device Monitor Server Setup Recommendations". If you select **User**, specify Windows domain account name and password. Name is entered in DOMAIN\USERNAME format.
Click **Next**.

11. **Configuring server administrator account**

Provide credentials (username and password) for server administrator account. This will be a **Super user** account (for further details, see "*InfoWatch Traffic Monitor. User Guide*", "Managing Console Accounts" section): it is used when you first connect to the server from Management Console.

Click **Next**.

12. **Configuring InfoWatch Traffic Monitor connection parameters**

If at step 4 you decided to use an existing database (**Install New Database** option was not selected), then this step will be skipped.
Specify InfoWatch Traffic Monitor interaction options:

- **TM server address**. InfoWatch Traffic Monitor server address. Address must be entered in the following format:

  `host:port`
  Host parameter should contain domain name or IP address of InfoWatch Traffic Monitor server. The server address is the standard URI address (Uniform Resource Identifier) with its formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.
  Port parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 9100.

  Important!

  If you are going to integrate Device Monitor with Traffic Monitor 5.5 or earlier use format: `host:port`, where `port - 4101`.

- **Number of connections**. Number of InfoWatch Traffic Monitor server connections. You can specify from 1 to 32 connections.
- **Authorization token**. The token used for API connection. Required for Traffic Monitor v. 6.0 or higher. Please get this token from Traffic Monitor administrator.

- If Device Monitor deployment scheme is not integrated with InfoWatch Traffic Monitor, select **Work in standalone mode** box. In this case, you can save captured shadow copies in server installation directory by selecting **Save shadow copies** box.

Click **Next**.

13. **Completing the installation**

Click **Install** to start Server installation.

During installation, the allowance to install Taiga system software will be requested. The allowance is needed to install drivers providing the support of mobile devices control. Click **Install**: otherwise the Wizard will finish its work prematurely and rollback the installation.

Important!

This message will appear if at Step 3 "Selecting Components to Install" you have selected the **MSM module (Taiga)** component.

Follow the instructions to complete installation.

Important!

Installing server end on Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2, you will see **Windows Security** dialog window, which installs InfoWatch virtual printer, required for processing printer jobs from metro-applications. To install virtual printer press **Install**.

Note:

Signature installation may take a while (up to 30 minutes).

3.6.2 InfoWatch Device Monitor Client Installation

InfoWatch Device Monitor Client can be installed on workstations in the following ways:

- Local Installation. It uses the Setup Wizard on each computer.
- Remote installation using third-party software. It uses software distribution tools: for example, Microsoft Active Directory group policy.
- Remote installation through InfoWatch Device Monitor Management Console expansion tasks (for details, see "*Infowatch Traffic Monitor. User Guide",* "Clients Remote Installation, Updating and Uninstallation" section).

InfoWatch Device Monitor Client is installed on mobile devices when adding this device to the security scheme (for details, see "*Infowatch Traffic Monitor. User Guide",* "Adding a Mobile Device through Appointment to Employee" and "Adding a Mobile Device to Computer Group" articles).

Important!

Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

Important!

For InfoWatch Device Monitor Client proper operation on computers with antivirus software installed, please disable antivirus self-protect function.

Important!

During the Client installation, the Mozilla Firefox and Mozilla Thunderbird applications (if they were running) will be closed.

3.6.2.1 Standard Client Installation

Important!

It is not recommended to install InfoWatch Device Monitor Clients on computers that have the same name. These computers will be registered as a single computer, affected by the same policies, and register the same events, etc.

Client can be installed by computer's local administrator.

1. **Running the Installation Wizard**

   Insert the installation CD into your CD-ROM drive. Then open `Client` directory. Run platform-specific setup file from this directory.
   You will be redirected to InfoWatch Device Monitor Client Installation Wizard welcome screen. Click **Next** to go to the next installation screen.

2. **Choose installation directory**

   Specify the path to Client installation directory.

Important!

Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the client installation will be incorrect.

Click **Next**.

3. **Configuring settings**

   Specify InfoWatch Device Monitor server connection settings:

   - **Server**. InfoWatch Device Monitor server name.
   - **Port**. Port number used for communication between InfoWatch Device Monitor Client and Server (port 15101 by default).

   Click **Next**.

4. **Completing the installation**

   Proceed to **Confirm installation** screen and click **Next** to start Client installation. Follow the instructions to complete the installation. Restart your computer to finish the installation.

3.6.2.2 Client Installation via Software Distribution Tools

Corporate network administrator can perform Client centralized setup via software distribution tools. This section describes installation from Microsoft Active Directory.
Client installation from Microsoft Active Directory is carried out via group policy. To do so, you have to select a group policy that covers all target workstations. This policy may be assigned to:

- Active Directory container that holds all target workstations
- the whole Active Directory domain, but not default domain policy. This policy should only cover the group that includes all controlled workstations.

1. **Creating Installation Package**

   Create `Client.en.msi` installation package as described in "*Infowatch Traffic Monitor. User Guide*", "Creating Installation Package" article). Put the installation package to the network directory that can be ready by all target computers within the domain.

2. **Disable Microsoft Windows XP Professional fast logon option**

   Before you start client setup via group policies, disable fast logon optimization for computers with Microsoft Windows XP Professional OS (so-called asynchronous logon mode). For more details on this functionality see Microsoft Knowledge Base (see KB305293).

   To disable the fast logon optimization feature:

   a. Open the group policy editor.

   b. In console tree, select **Computer Configuration** > **Administrative templates** > **System** > **Logon**. In details section, select **Always wait for the network at computer startup and logon**. Then set the value of this parameter to **Enabled** in properties screen.

> **Note:**
>
> If this option has been turned off, you will need to reboot your computer again to let Windows group policy distribution mechanism finishes the installation.

3. **Editing Group Policy**

Edit group policy before installing Client from Active Directory.
To edit group policy:

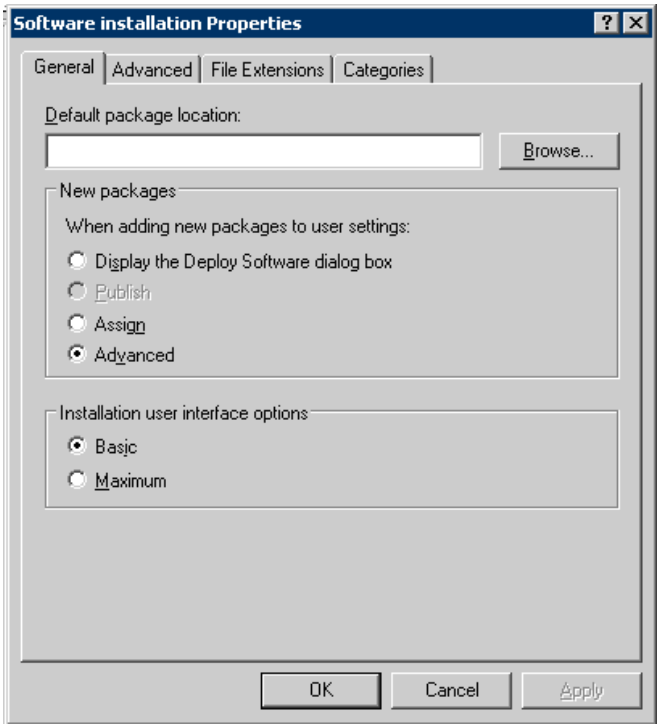
a. Open **Active directory users and computers** (**Start** > **Settings** > **Control Panel** > **Administrative tools** > **Active directory users and computers**).

b. In the console tree, select Active Directory container with all target workstations.

c. Open **Group Policy**. To do this, click **Properties** in Active Directory container context menu. In the following dialog box, navigate to **Group policy** tab. On this tab, select group policy and click **Edit**.

d. In the console tree, select **Software Installation** (**Computer Configuration** > **Software Settings**).

e. In **Software Installation** context menu select **Properties**. On General tab configure the following settings (see the picture below):
- set **New packages** value to **Advanced**;
- set **Installation user interface options** value to **Basic**.



f. When the configuration is complete, click **OK**.

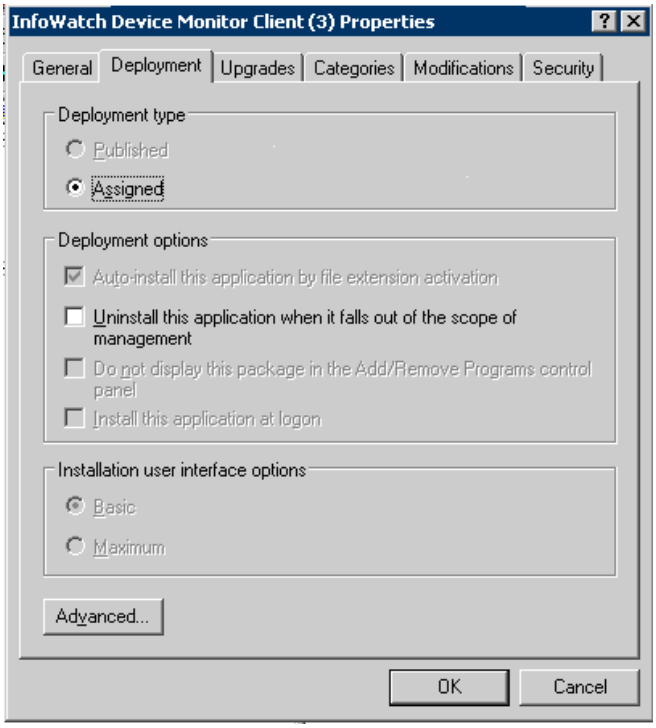
4. **Preparing Client installation task**

   Client installation task is created and configured on **Group Policy Object Editor** screen:

   a. After opening **Group Policy Object Editor** box select **Software Settings** (**Computer Configuration** > **Software Settings**) in the console tree. Right-click the selected item and then select **New** > **Package**.

   b. In the following **Open** dialog specify client module installation package `Setup.Client.msi` (first move the installation package to a network directory that is readablefor all installation-target computers within the domain).

   c. Configure new package properties:
   - Make sure all settings in **Deployment** tab comply with the following figure.



   - After all necessary settings have been configured, click **OK**.

   d. In the console tree, select **Computer Configuration** > **Administrative templates** > **System** > **Scripts**. In details section, select **Run logon scripts synchronously**. Then set the value to **Enabled** in properties screen.

5. **Setup**

   New task appears in **Software Installation** task list. The task is carried out as soon as the target computer is restarted. InfoWatch Device Monitor Client starts automatically after its installation. Installation method is displayed in **Deployment state** column. **Assigned** status means that installation is forced, i.e. doesn't need approval of target computer user. **Published** state means installation upon user's approval.

Important!

You can check if the Client has been installed successfully in InfoWatch Device Monitor Management Console. All workstations the Client has been successfully installed to must appear in the list in **Workstations** area. To view all managed workstations, click **Show all workstations** at the top of Navigation Pane. To obtain up-to-date Client information, click **Update** in Toolbar.

If computer is not in the list, check for "*Group policy application failure on Windows XP with Service Pack 2 (SP2) computer*" error. For error description and troubleshooting go to Microsoft website: https://support.microsoft.com/en-us/kb/840669.

4 UPDATING THE SYSTEM

Note:

On information how to update Device Monitor Server and Clients, see "Updating InfoWatch Device Monitor".

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

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 the default

transport mode - the copy mode. If you need to use the blocking mode (in-line), then, in the `system.lua` configuration file, replace **Copy** value of the **transport_mode** setting with **Normal** one. For details on configuring the transport mode, see "*InfoWatch Traffic Monitor. Administration Guide*", "Configuring Traffic Interception" section, subsections for needed traffic types.

.

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. Stop all iwtm services:
   `service iwtm stop`
9. Install the `iwtm-tmcap`:

   ```
   yum install iwtm-tmcap
   ```
10. Run packages update process:
    - if you run Oracle DBMS, use command `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg`
    - if you run PostgreSQL DBMS, use command `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle`
11. 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.
12. 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.
13. 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. 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.

2. Switch to user: `su - oracle`.

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

3. 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.
4. Go to directory `/opt/iw/tm5/csw/oracle`:

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

5. Run database update with a script:

   ```
   ./update.sh
   ```

6. Clear cache on the server where `web-gui` is installed using the following command:

   ```
   redis-cli flushall
   ```

7. Start the stopped services (one needs to switch back to **root** user):

   ```
   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. 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.

2. Switch to user: `su - postgres`.

Note:

Default schema owner login is `iwtm`.

3. 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.
4. Go to directory `/opt/iw/tm5/csw/postgres`:

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

5. Run database update with a script:

   ```
   ./update.sh
   ```

6. Clear cache on the server where web-gui is installed using the following command:

   ```
   redis-cli flushall
   ```

7. Start the stopped services (one needs to switch back to **root** user):

   ```
   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").

4.4 Updating InfoWatch Device Monitor

If you have InfoWatch Device Monitor installed, you can upgrade it to a later version.

System update is similar to its installation:

1. Updating InfoWatch Device Monitor Server End (database, server, and Management Console).

Important!

If you want to upgrade System version 3.4 - 4.0, delete the old server version (don't remove the database) and re-install the server, configuring the connection to existing database. Starting version 4.0, updates use the standard procedure.

2. Updating InfoWatch Device Monitor Client.
   Device Monitor supports earlier Client versions starting build 3.4.875. Therefore, Client is upgraded when needed.

Important!

When upgrading Device Monitor version 6.0 by deleting and then installing the Server, you must perform the following actions to let Device Monitor Clients to connect to the new Server:

1. When deleting - save encryption key stored in DM Server installation folder, `SSLServerKey.pfx` file.

2. When installing - specify the path to the saved encryption key used on the old Server.

4.4.1 Updating InfoWatch Device Monitor Server End

Important!

If you want to upgrade Device Monitor version **3.4** - **4.0**, delete the old server version (don't remove the database) and re-install the server, configuring the connection to existing database.

Starting from version **4.0**, the upgrading is fulfilled in the standard way.

When upgrading the System version **6.0** by deleting and then installing the Server, you must perform the following actions to let Device Monitor Clients to connect to the new Server:

1. When deleting - save encryption key stored in DM Server installation folder, `SSLServerKey.pfx` file.
2. When installing - specify the path to the saved encryption key used on the old Server.

4.4.1.1 Step 1. Start update

Insert the installation CD into your CD-ROM drive. Then open Server directory. Run platform-specific setup file from this directory.

You will be redirected to InfoWatch Device Monitor Installation Wizard welcome screen. Click **Next** to go to the next installation screen.

4.4.1.2 Step 2. Accepting the License Agreement

Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms** in **the License Agreement** and click **Next**.

4.4.1.3 Step 3. Database configuration

Database is preserved during update, and **Configure Database Connection** box automatically displays old database parameters. However, depending on DBMS, you need to specify particular settings.

Built-in Database Update

Skip this step if you are using built-in DB.

Update Database Under Microsoft SQL Server DBMS

On **Authentication Method** panel, select authentication method for the user, who updates the database. For this option, specify the authentication method selected during account preparation (see "Database deployment under Microsoft SQL Server DBMS").

If the account uses Windows authentication, select **Windows authentication**.

If the account uses built-in SQL Server authentication, select **SQL Server built-in**. Then enter login and password into **User name** and **Password** fields respectively.

> **Note:**
>
> You can specify old or new authentication parameters as the upgrade proceeds. For guidelines on authentication methods and account preparation see section "Database deployment under Microsoft SQL Server DBMS".

Update Database Under Oracle DBMS

On **DB Server** panel, specify **Password for 'SYSTEM'** - password for SYSTEM account that manages the database, which is being updated.

On **Scheme Information** panel, fill in **Password**, **Confirm password** fields - password for database scheme owner's account used for database update.

Update PostgreSQL Database

Enter the password of the account that manages the updated database into **Password** field.

After you have configured all parameters, click **Next**.

4.4.1.4 Step 4. Upgrade Completion

Go to the next screen and click **Install** to run System server upgrade.

Follow Setup Wizard's instructions to complete System server update.

4.4.2 Updating InfoWatch Device Monitor Client

The system supports Client versions starting from build 3.4.875. Therefore, updated system components can work with older Client versions. However, you can update to a later version.

Client update is similar to its installation:

- local update using Setup Wizard;
- remote update using software distribution tools;
- centralized update via Management Console (for details, see "*InfoWatch Traffic Monitor. User Guide*", "Creating Update Task" article).

In case you need to update Device Monitor Client on a large number of Workstations, you need to take the following steps:

1. Update client on a group of 10 Workstations. Make sure that there are no performance errors for 2-3 days.
2. Update client on a group of 50 Workstations. Make sure that there are no performance errors for 2-3 days.

3. Update client on a group of 500 Workstations. Make sure that there are no performance errors for 2-3 days.
4. Update client on a group of 1000 Workstations. Make sure that there are no performance errors for 2-3 days.
5. Complete the update procedure with the rest of the Workstations.

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".
- See details on Device Monitor removal (Server and Clients) in "Uninstalling InfoWatch Device Monitor".
- 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 Traffic Monitor server components (Management console, Sniffer, IW ICAP, remote database interaction module, and the others) can be deleted using 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 the 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, the following entities are left on the computer:

- the 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.

Important!

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

1. **Checking the Oracle DBMS**

   Make sure that:

   - the version of the 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 an account having SYSDBA permissions are specified correctly (values of parameters `sysdba` and `sysdba_password`).

2. **Stopping 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

Important!

When deleting the database scheme, the following components are also deleted from the System:

- Policies, including preinstalled ones (see "*Infowatch Traffic Monitor. User guide*", "Preinstalled Policies" article).
- Plugins and tokens (see "*Infowatch Traffic Monitor. Administration guide*", "Plugins" article).

To restore Device Monitor plugin and redeploy preinstalled policies:

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

Then you need to manually add other plugins (see "*Infowatch Traffic Monitor. Administration guide*", "Adding plugin" article) and create required policies (see "*Infowatch Traffic Monitor. User guide*", "Creating Data Protection Policy" and "Creating Person Control Policy" articles).

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.

5.3 Uninstalling InfoWatch Device Monitor

Important!

If you are planning to install the Device Monitor Server again, then to make Device Monitor Clients could connect and bind to the new server, then starting from version 6.0 you must save the encryption key of the old server.

The encryption key is stored in the installation folder of the InfoWatch Device Monitor Server, `SSLServerKey.pfx` file.

To remove InfoWatch Device Monitor server end with Management Console:

1. Take one of the following steps:
   - Open `Setup\Unified` catalog on the Installation CD. Run platform-specific setup file from this directory.
   - Run **Uninstall or remove programs** from Windows Control Panel, select **InfoWatch Device Monitor** and click **Change**.
2. On **Change, repair or remove…** screen select **Remove**.
3. To remove the system and its database, flag **Remove database** on **Remove database...** screen. Then specify parameters for uninstalling: parameters depend on your DBMS:
   - **Integrated DB (CompactSQL)** – doesn't require additional parameters: **Database** string contains the removed DB file.
   - **Microsoft SQL Server** – specify your authentication method by selecting it in Authentication Method pane (see "Database deployment under Microsoft SQL Server DBMS").
     In case of SQL-server based authentication (**Integrated into SQL Server**) enter the credentials you used to connect to the database in **Login** and **Password** boxes of **Database Administrator** pane.
   - **Oracle** – enter the password into **The password of 'SYSTEM' login** box. This will remove database scheme owner account and all its objects except the tablespace.
   - **PostgreSQL** –enter the credentials used to create the DB during server setup into User name and Password boxes (see "InfoWatch Device Monitor Server End Installation Procedure").

Important!

If the database is not working or working partially, then to delete the InfoWatch Device Monitor you should uncheck the **Remove database** field, otherwise the deletion can be performed incompletely.

4. After specifying the parameters click **Next** and then click **Remove** to start uninstallation.

To remove only InfoWatch Device Monitor server end or Management Console:

1. Run **Add or remove programs** and click **Change**.
2. In **Custom Setup** click  to the left of the elements you want to remove and select **Disable this element**. Click **Next**.
3. If you selected server uninstallation at the previous step, specify whether you want to remove the database and enter the authorized account parameters, if necessary, on **Remove database…** screen (see details above).
4. Click **Change** to start uninstallation.

To remove InfoWatch Device Monitor Client:

run **Add or remove programs**, select **InfoWatch Device Monitor Client** and click **Remove**.

You can also use centralized uninstallation to remove Clients:

- with Active Directory tools (if Clients were installed via software distribution tools) as described in "Remove Client Installed via Software Distribution Tools".
- with Management Console distribution tasks (for details, see "*InfoWatch Traffic Monitor. Administration Guide*", "Clients Remote Setup, Updating and Uninstallation" section).

Important!

Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

The order of deleting the Clients from mobile devices is described in "*InfoWatch Traffic Monitor. Administration Guide*", "Deleting the Mobile Device" article.

5.3.1 Remove Client Installed via Software Distribution Tools

If client was installed via software distribution tools, you can use them to remove it.

For example, if Clients were installed via Microsoft Active Directory, corporate network administrator can use group policy to remove the installation task. Group policy editing procedure is described in "Client setup via software distribution tools", step 3.

To remove Client from all managed workstations:

1. Select the installation task you want to remove. Then right-click the selected row and select **All tasks** > **Remove**.

2. Select **Remove software** in **Immediately uninstall software from users and computers** dialog.

> **Note:**
>
> Other options remove installation task without uninstalling all existing Clients. After that you won't be able to remove these Clients with Microsoft Active Directory tools.

3. Click **OK**.

Client will be removed from all computers under selected group policy.

6 APPENDIX A. USERNAME AND PASSWORD RECOMMENDATIONS

Requirements for usernames

- The username 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: «#», «$» or «_».
  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