INFOWATCH

InfoWatch Traffic Monitor 5.5

Installation guide

INFOWATCH TRAFFIC MONITOR 5.5

Installation guide

© ZAO “InfoWatch”
Tel/Fax +7 (495) 229-00-22
http://www.infowatch.com

Revision date: 24/04/2015

TABLE OF CONTENTS

INTRODUCTION 5
Who Should Read this Guide 5
Guide Structure 5
Additional Documentation 5
General Conventions 6
Technical Support 6

CHAPTER 1. GETTING READY TO INSTALL 7
1.1. System Deployment Schemas and choosing installation type 7
1.1.1. SMTP Traffic 7
1.1.1.1. SPAN, or Port Mirroring 8
1.1.1.2. Receiving copies from Mail Server 9
1.1.1.3. Inline mode 9
1.1.2. HTTP Traffic 9
1.1.2.1. SPAN, or Port Mirroring 9
1.1.2.2. Inline mode 10
1.1.3. HTTPS Traffic 11
1.1.3.1. Inline mode 11
1.1.4. ICQ Traffic 11
1.1.4.1. SPAN, or Port Mirroring 11
1.1.5. NRPC Traffic 12
1.1.5.1. SPAN, or Port Mirroring 12
1.1.6. Receiving Objects Intercepted by InfoWatch Device Monitor 12
1.1.7. Receiving Files from the Corporate Network 13
1.1.8. Objects Obtained from DeviceLock 13
1.1.9. Objects Obtained from MS Lync 13
1.2. Hardware and software requirements 13
1.2.1. Disk Subsystem 14
1.2.2. Processor 14
1.2.3. Random access memory 14
1.2.4. Sniffer 14
1.2.5. IW ICAP Module 15
1.2.6. IW Crawler 16
1.2.7. InfoWatch Lync Adapter 16
1.2.8. Management Console 17

CHAPTER 2. SYSTEM INSTALLATION 18
2.1. Server Components Installation 18
2.1.1. Major Information about Installation Steps 19
2.1.1.1. Start Window 19
2.1.1.2. Timezone Specification 20
2.1.1.3. System Superuser Password Creation 20
2.1.1.4. Choosing Disk Layout 21
2.1.1.5. Network Settings 23
2.1.1.6. DB Language Choice 24
2.1.1.7. Configuring Timezone Synchronization (NTP-Server) 25
2.1.1.8. Installation Completion 26

2.1.2. Installation from TME Package 26
2.1.2.1. "All-in-one" Installation Mode (IWALLX) 27
2.1.2.2. Database Installation (IWDBX) 33
2.1.2.3. Traffic Monitor server installation (IWTMX) 35
2.1.3. Installation from TMS Package 37
2.2. Web-Console Installation 43
2.3. Crawler Subsystem Installation 44
2.4. Installing the InfoWatch Lync Adapter 48
2.4.1. Installing the InfoWatch Transfer Service 1.0 48
2.4.2. Installing the IW OCS Filter 2.0 50

CHAPTER 3. UPDATING THE SYSTEM 52
3.1. Updating RHEL and IWTM packages 52
3.2. Updating DB scheme 53

CHAPTER 4. UNINSTALLING THE SYSTEM 56
4.1. Database Schema 56
4.2. Remote Database Management Module 57
4.3. IW ICAP Module 57
4.4. Traffic Monitor Server 57
4.5. Sniffer 58
4.6. Crawler 58
4.7. Web-console 58
4.8. InfoWatch Lync Adapter 58

APPENDIX 1. USER NAME AND PASSWORD RECOMMENDATION 59

APPENDIX 2. THIRD-PARTY LICENSES 61

GLOSSARY 62

INTRODUCTION

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

Who Should Read this Guide

The guide is intended for users with the following skills:

- Administration of Oracle DBMS
- Installation and Configuration of Red Hat Enterprise Linux and its configuration files management
- Working with Microsoft Windows

Guide Structure

In this guide you can find information about the following topics:

- *Chapter 1. Getting Ready to Install (page 7).*

  Description of installation types, hardware and software requirements.

- *Chapter 2. System Installation (page 18).*

  This chapter contains recommendations for installing System components and describes the installation process.

- *Chapter 3. Updating the System (page 52).*

  This chapter contains a description of System update process with the help of the update package supplied on the distribution disk.

- *Chapter 4. Uninstalling the System (page 52).*

  This chapter provides information on how to uninstall components of the System.

- *Appendix 1. User name and password recommendation (page 59).*

  This appendix contains a list of rules to create user passwords and recommendations for safe password creation.

- *Appendix 2. Third-Party Licenses (page 61).*

  This appendix contains license agreements for third-party software components of this System.

Additional Documentation

For more information, see the following documents:

- *"InfoWatch Traffic Monitor. User Guide".*

  This document describes how to use InfoWatch Traffic Monitor (configuring, importing/exporting data, creating object processing rules).

- *"InfoWatch Traffic Monitor. Administration Guide"*

  This document describes how to administrate the System (database, server part).

- "*InfoWatch Device Monitor. User Guide"*

  This document describes the principles of working with InfoWatch Device Monitor.

General Conventions

This document contains different types and styles to bring your attention to specific information. The following table explains where these styles are applied.

Style	Description	Example
Bold	Bold indicates GUI elements (buttons, menu commands, etc.), system components (if they are mentioned for the first time in the document).	The **iw_qtool** utility is used to move objects form one queue to another.
Italics	Italics indicate tables, examples and descriptions, specifically the names and values of object attributes.	The content filtering database contains the *Contract* term
`The Courier New font`	The font indicates file names, program code examples, values of configuration files parameters, examples of settings.	To verify that Traffic Monitor Server is running use the following commands: `service iwtm status`
`The COURIER NEW font(UPPER CASE)`	This font is used in the descriptions of configuration files and indicates file sections (in square brackets), variables and parameters. When used in database description, it indicates SQL keywords, PL/SQL instructions, data types and privileges	The autorun parameters are specified in `/opt/iw/tm5/etc/sniffer.conf` file, `[STARTUP]` section

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 on 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.

CHAPTER 1. GETTING READY TO INSTALL

1.1. System Deployment Schemas and choosing installation type

The following types of installing InfoWatch Traffic Monitor are available:

- *All-in-one Enterprise* – All system components (with Oracle Enterprise DBMS) are installed on the same server. This type of installation is normally used if the server is powerful enough to enable operation of both Oracle DBMS (Enterprise) and Traffic Monitor services;
- *Traffic Monitor Server* + Database – Traffic Monitor Server and Oracle DBMS Enterprise are installed on different computers. This installation type is used when capacity of one server is not enough to enable operation of both Traffic Monitor services and Oracle DBMS (Enterprise);
- *All-in-one Standard* – All system components (with Oracle Standard DBMS) are installed on the same server. This type of installation is normally used if the server is powerful enough to enable operation of both Oracle DBMS (Standard) and Traffic Monitor services;

Find description on what installation types to choose depending on the type of traffic being intercepted and the way of interception:

- *SMTP Traffic (i. 1.1.1 on page 7)*
- *HTTP Traffic (i. 1.1.2 on page 9)*
- *HTTPS Traffic (i. 1.1.3 on page 11)*
- *ICQ Traffic (i. 1.1.4 on page 9)*
- *NRPC Traffic (i. 1.1.5 on page 12)*
- *Receiving Objects Intercepted by InfoWatch Device Monitor (i. 1.1.6 on page 12)*
- *Receiving Files from the Corporate Network (i. 1.1.7 on page 13)*
- *Objects Obtained from DeviceLock (i. 1.1.8 on page 13)*
- *Objects Obtained from MS Lync (i. 1.1.9 on page 13)*

> **Warning!**
>
> After installation, administrator should configure the System depending on introduction purposes (see «*InfoWatch Traffic Monitor. Administration guide*»).

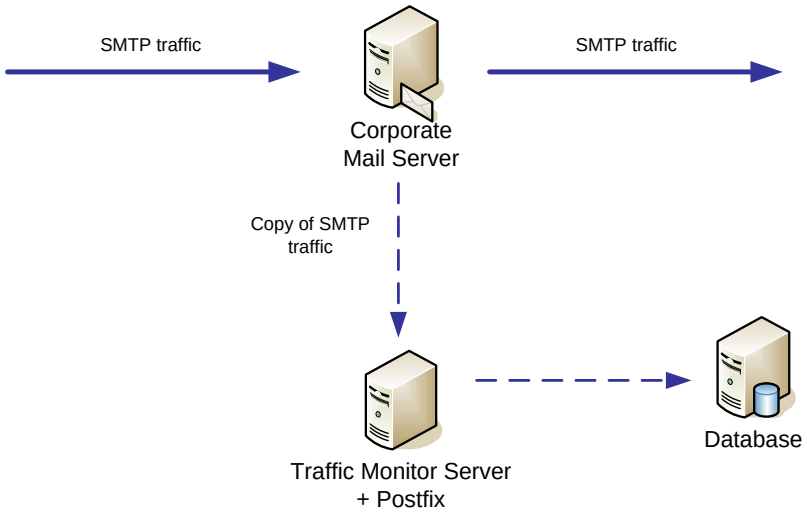
1.1.1. SMTP Traffic

SMTP Traffic can be intercepted by following means:

- SPAN, or Port Mirroring
- Receiving copies from Mail Server
- Inline mode

1.1.1.1. SPAN, or Port Mirroring

Variant 1. Interception and traffic type analysis is being performed on one Computer, clusters are not used



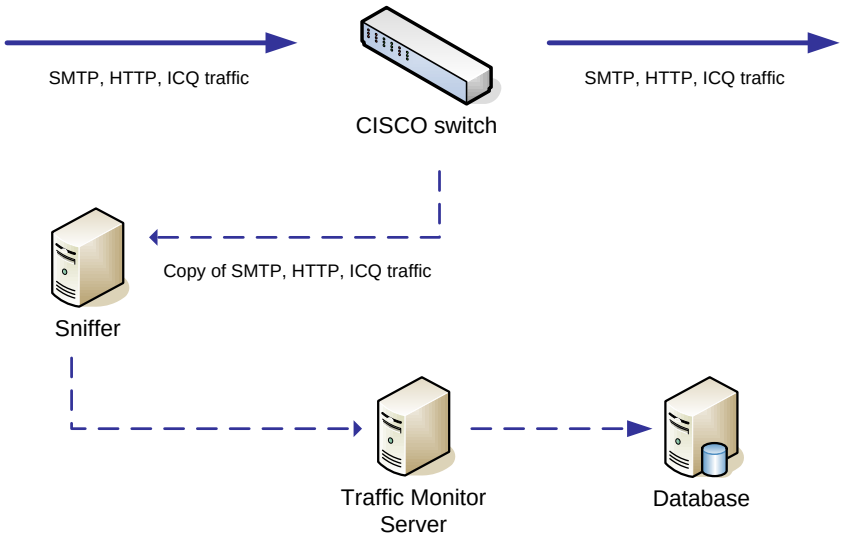
Possible installation types:

- All-in-one Enterprise (see i. 2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

Variant 2. A copy of traffic is intercepted and analyzed on different computers; clusters are not used.



Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

Variant 3. A copy of traffic is intercepted and analyzed on different computers. To improve performance, a cluster with 2 instances of Traffic Monitor Server is created.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

1.1.1.2. Receiving copies from Mail Server

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

1.1.1.3. Inline mode

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

1.1.2. HTTP Traffic

HTTTP Traffic can be intercepted by following means:

- SPAN, or Port Mirroring
- Inline mode

1.1.2.1. SPAN, or Port Mirroring

Variant 1. Interception and traffic type analysis is being performed on one Computer, clusters are not used.

Possible installation types:

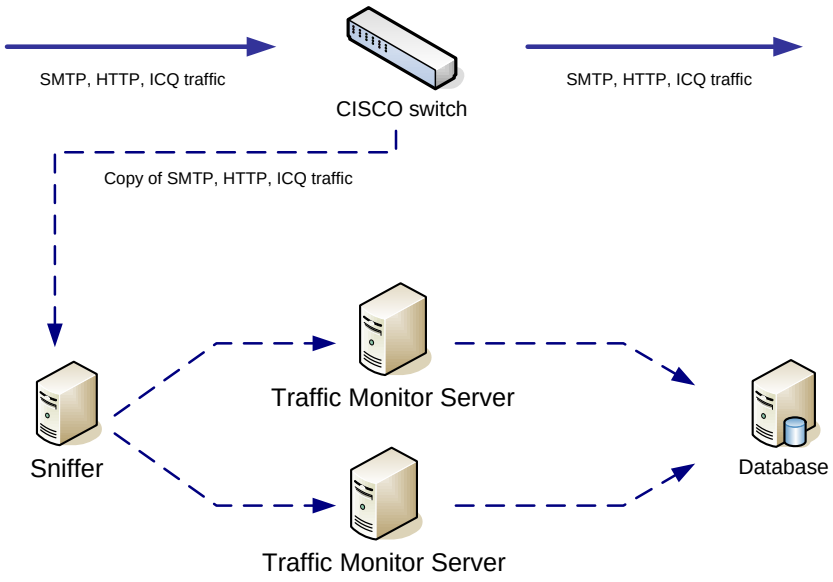
- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

Variant 2. A copy of traffic is intercepted and analyzed on different computers; clusters are not used.

Possible installation types:



- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or

- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

Variant 3. A copy of traffic is intercepted and analyzed on different computers. To improve performance, a cluster with 2 instances of Traffic Monitor Server is created.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or

- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

1.1.2.2. Inline mode

Possible installation types:

- All-in-one Enterprise (see i. 2.1.2.1 on page 27)

  or

- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or

- All-in-one Standard (see i. 2.1.3 on page 37)

1.1.3. HTTPS Traffic

Https can be intercepted only in a way described below.

1.1.3.1. Inline mode

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

1.1.4. ICQ Traffic

ICQ traffic can be intercepted only in a way described below.

1.1.4.1. SPAN, or Port Mirroring

Variant 1. Interception and analysis of a traffic copy are performed on the same computer, clusters are not used.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

Variant 2. A copy of traffic is intercepted and analyzed on different computers; clusters are not used.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

Variant 3. A copy of traffic is intercepted and analyzed on different computers. To improve performance, a cluster with 2 instances of Traffic Monitor Server is created.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

1.1.5. NRPC Traffic

NRPC traffic can be intercepted only in a way described below.

1.1.5.1. SPAN, or Port Mirroring

Variant 1. Interception and analysis of a traffic copy are performed on the same computer, clusters are not used.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

Variant 2. A copy of traffic is intercepted and analyzed on different computers; clusters are not used.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

Variant 3. A copy of traffic is intercepted and analyzed on different computers. To improve performance, a cluster with 2 instances of Traffic Monitor Server is created.

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

1.1.6. Receiving Objects Intercepted by InfoWatch Device Monitor

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or
- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or
- All-in-one Standard (see i. 2.1.3 on page 37)

1.1.7. Receiving Files from the Corporate Network

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or

- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or

- All-in-one Standard (see i. 2.1.3 on page 37)

1.1.8. Objects Obtained from DeviceLock

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or

- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or

- All-in-one Standard (see i. 2.1.3 on page 37)

1.1.9. Objects Obtained from MS Lync

Possible installation types:

- All-in-one Enterprise (see i.2.1.2.1 on page 27)

  or

- Traffic Monitor Server (see i. 2.1.2.3 on page 35) + Database (see i. 2.1.2.2 on page 33)

  or

- All-in-one Standard (see i. 2.1.3 on page 37)

1.2. Hardware and software requirements

Hardware configuration requirements of server and DBMS for **Traffic Monitor Enterprise** are defined based on selected deployment schema and parameters of the network where the System is installed. For this reason, equipment specification is determined individually in each case.

> **Warning!**
>
> For Traffic Monitor Enterprise the Traffic Monitor server and Oracle DBMS Server must be installed on different computers. In this case you shouldn't install or run applications (especially server applications), or use this computer as a file server on the computer acting as Oracle DBMS server.

Hardware and software requirements are listed in the following chapters:

- Disk Subsystem (see i. 1.2.1 on page 14);
- Processor (see i. 1.2.2 on page 14);
- Random access memory (see i. 1.2.3 on page 14);
- Sniffer (see i. 1.2.4 on page 14);
- IW ICAP Module (see i. 1.2.5 on page 15);

- IW Crawler (see i. 1.2.6 on page 16);
- InfoWatch Lync Adapter (see i. 1.2.7 on page 16);
- Management Console (see i. 1.2.8 on page 17);

1.2.1. Disk Subsystem

Requirements for the subsystem can differ depending on the System version.

Disk subsystem parameters for *InfoWatch Traffic Monitor Enterprise*:

Less than 10 GB/Day	From 10 GB/Day To 50 GB/Day	From 50 GB/Day to 100 GB/Day	More than 100 GB/Day
SATA, 600GB	SATA/SAS, RAID5, 6+ HDD	SAS	SAS

InfoWatch Traffic Monitor Standard disk subsystem should have not less than 400GB capacity regardless of its load.

1.2.2. Processor

The following processor requirements are submitted depending on the System load:

Less than 10 GB/Day	From 10 GB/Day to 50 GB/Day	From 50 GB/Day to 100 GB/Day	More than 100 GB/Day
2CPU 8xC + Hyper-threading	*2SRVx2CPU 10xC*	*Calculated on request*	*Calculated on request*

1.2.3. Random access memory

The following RAM requirements are submitted depending on the System load:

Less than 10 GB/Day	From 10 GB/Day to 50 GB/Day	From 50 GB/Day to 100 GB/Day	More than 100 GB/Day
32GB	64GB	64GB for each server	64GB for each server

1.2.4. Sniffer

Network Equipment Requirements

Sniffer may receive a copy of traffic from the switch that supports SPAN (recommended model – Cisco Catalyst 2960 Series).

After switch is installed, configure SPAN port to operate in RX/TX mode as described in technical documentation of the switch.

Hardware requirements

Minimum requirements for traffic up to 10 GB/Day:

- Processor: quad-core HP DL360p Gen8 E5-2603 Entry EU Svr (2,6Ghz)
- RAM: 8 GB.

The standard configuration of the Sniffer when the aggregate speed of upstream and downstream is 100 Mbit/s:

- Server: support configurations, allowed for the Red Hat Enterprise Linux Server 6: see https://hardware.redhat.com/.

  The recommended configuration is quad-core HP DL360p Gen8 E5-2603 Entry EU Svr (2,6Ghz).
- RAM: 8 GB DDR3
- Hard drive: SAS 500 GB (10000 rpm).

Network adapter requirements:

General requirements	Recommended network adapters
NAPI and *Promiscuous mode* support	Intel Corporation 82540EM Gigabit Ethernet Controller
Gigabit Ethernet support	Intel PRO/1000 GT network adapters are allowed

The Sniffer should have at least two network cards installed:

- A network adapter to receive a copy of traffic from one SPAN port of the CISCO switch. If traffic is received from multiple SPAN ports (and ports can be configured both on the same switch and on different switches), then a separate network adapter is required for each of the SPAN ports.
- A network adapter to interact with other network objects. Specifically, this adapter is required to send traffic to Traffic Monitor server or interact with the database (if Sniffer and Traffic Monitor server are installed on the same computer).

1.2.5. IW ICAP Module

If the IW ICAP module is integrated with the System, HTTP requests are transmitted over a proxy server. An ICAP client is required to send HTTP requests to Traffic Monitor server over ICAP protocol. The System supports ICAP clients integrated with the proxy server.

> **Warning!**
>
> Traffic Monitor Server and proxy with ICAP client should be located in the same subnetwork to simplify configuration process.

The following proxy-servers are supported:

- SQUID no lower than 3.2.1 with ICAP support enabled.
- Cisco IronPort S10.
- Blue Coat SG Series with ICAP license. Some models which are currently produced by Blue Coat Systems are supported. The manufacturer constantly updates the product range. Therefore, prior to using a specific model of Blue Coat Proxy SG, contact InfoWatch technical support service to check whether or not this model is compatible with the IW ICAP module.

  > **Note:**
  >
  > If interception of HTTPS traffic is required, configure proxy settings to process HTTPS traffic and send it to InfoWatch Traffic Monitor server as HTTP traffic.

See accompanying documentation for the selected proxy server for installation and configuration steps.

ICAP server is a part of ICAP integration module. The module is installed on the same computer as Traffic Monitor Server. There are no special requirements for hardware and software of the module.

1.2.6. IW Crawler

Requirements for InfoWatch Traffic Monitor server instance:

- 6 Gb RAM minimum
- the autorestart of `iw_expressd` process should be enabled (For more information on enabling process autostart see «*InfoWatch Traffic Monitor. Administration guide*»).

> **Warning!**
>
> Both Crawler server and Crawler scanner should be installed to computers located in the same domain: the one to which all workstations to scan are belong.

The computer, to which the **Crawler server** will be installed, should meet the following requirements:

- Processor: at least 2 cores
- RAM: 200 Mb free
- Hard drive: 1 Gb free
- OS:
  - Microsoft Windows XP / Vista / 7 / 8
  - Microsoft Windows Server 2003 / 2008 / 2012
- Microsoft .Net Framework 4.0

The computer, to which the **Crawler scanner** will be installed, should meet the following requirements:

- Processor: at least 2 cores
- RAM: 200 Mb free
- Hard drive: at least 10 Gb free for temporary storing files copied from reviewed resources
- OS:
  - Microsoft Windows XP / Vista / 7 / 8
  - Microsoft Windows Server 2003 / 2008 / 2012
- Microsoft .Net Framework 4.0
- Bandwidth of the network channel between Crawler scanner and Traffic Monitor server should be not less than bandwidth between Crawler scanner and scanned network nodes (workstations and file servers).

> **Warning!**
>
> We recommend to deploy a computer where Crawler scanner works so that it was located in the network segment maximally near to scanned segments. The distance from Crawler scanner to scanned objects can significantly increase network load.

> **Warning!**
>
> If network segments where InfoWatch Traffic Monitor with Crawler is deployed, are divided by firewalls, then for correct Crawler operation TCP ports **1337** (Traffic Monitor connects to Crawler server) and **6556** (Crawler scanner connects to Crawler server) should be opened.

1.2.7. InfoWatch Lync Adapter

For InfoWatch Lync Adapter to function properly, the following software is required:

- InfoWatch Traffic Monitor 5.4
- Microsoft Lync Server 2010 or Microsoft Lync Server 2013

Warning!

In case of integration with Microsoft Lync Server 2010, the following software is required to be installed:

- Service Pack 1 for Windows Server 2008 R2 or Service Pack 2 for Windows Server 2008
- Microsoft .NET Framework 4.5
- Windows PowerShell 3.0 or higher

1.2.8. Management Console

Starting from InfoWatch Traffic Monitor 5.1 the System uses Management Web-Console. The web-console operates on any hardware platform but requires internet-browser Google Chrome 30 or newer.

Hardware requirements

Software	Requirements
Internet-browser	Google Chrome 40 or newer Opera 27 or newer

CHAPTER 2. SYSTEM INSTALLATION

> **Note:**
>
> After system installation trial license will be already integrated into system (more information on licensing is available in document «*InfoWatch Traffic Monitor. Administration guide*»).

In the following chapter you will find instructions for each type of System installation.

Find more information on installation schemas and installation types in «*InfoWatch Traffic Monitor. Administration guide*».

> **Warning!**
>
> Before installation, make sure that environment of the System to be deployed matches software and hardware requirements.

2.1. Server Components Installation

InfoWatch Traffic Monitor server components installation is being performed with **kickstart** installation program.

> **Warning!**
>
> If the System is installed or updated without kickstart installation program (qualified InfoWatch engineers sometimes perform those operations) then you should specify Oracle environment by creating symbol link in the **/etc/profile.d/iw-oracle.sh** configuration file:
>
> - `/opt/iw/tm5/etc/iw-oracle_client.sh` – if Oracle DB is installed on the other computer;
> - `/opt/iw/tm5/etc/iw-oracle_server.sh` – if Oracle DB is installed on the same computer.

Detailed information on each installation type is available in the following chapters:

- Major Information about Installation Steps (see i. 2.1.1 on page 19);
- Installation from TME Package (see i. 2.1.2 on page 26);
- Installation from TMS Package (see i. 2.1.3 on page 37)

2.1.1. Major Information about Installation Steps

2.1.1.1. Start Window



Traffic Monitor Standard and Traffic Monitor Enterprise have different installation packages, first installation screen (**kickstart**) would be, as well, different.

Common parameters for both system types:

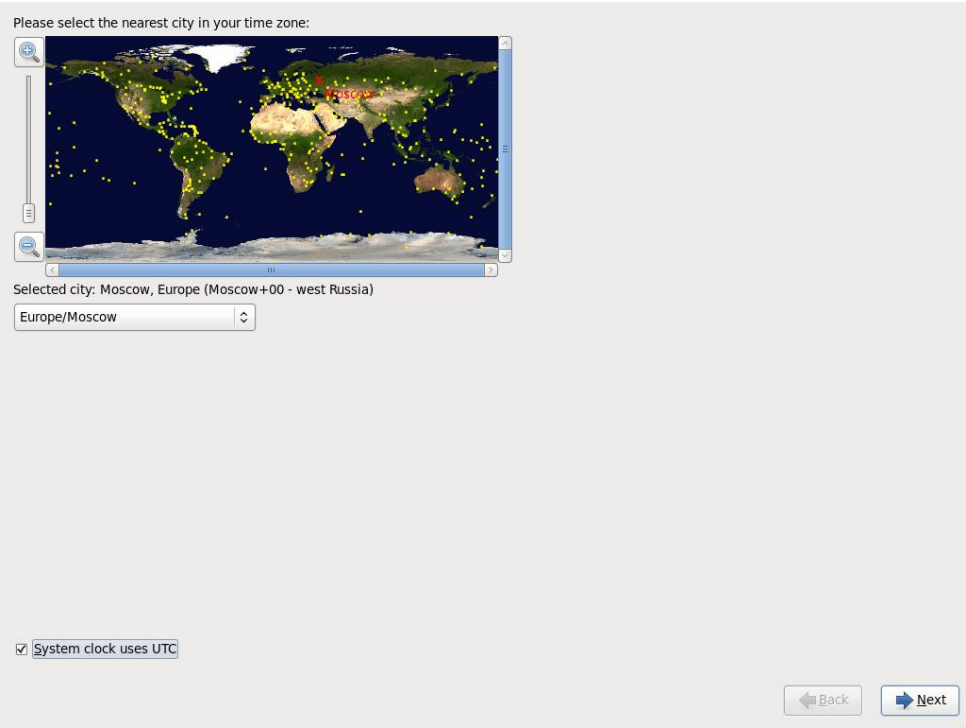
- **Boot from local drive** – load from local computer disk;
- **Rescue installed system** – emergency recovery of InfoWatch Traffic Monitor system. Used by InfoWatch engineers only;
- **Memory test** – hardware test (can take some time). Additional option used if necessary.

> **Note:**
>
> Press **F1** to review additional startup options.
>
> Due to further actions complexity, additional options are used only by InfoWatch engineers.

Installation types are present for:

- InfoWatch Traffic Monitor Enterprise (see i. 2.1.2 on page 26);
- InfoWatch Traffic Monitor Standard (see i. 2.1.3 on page 37)

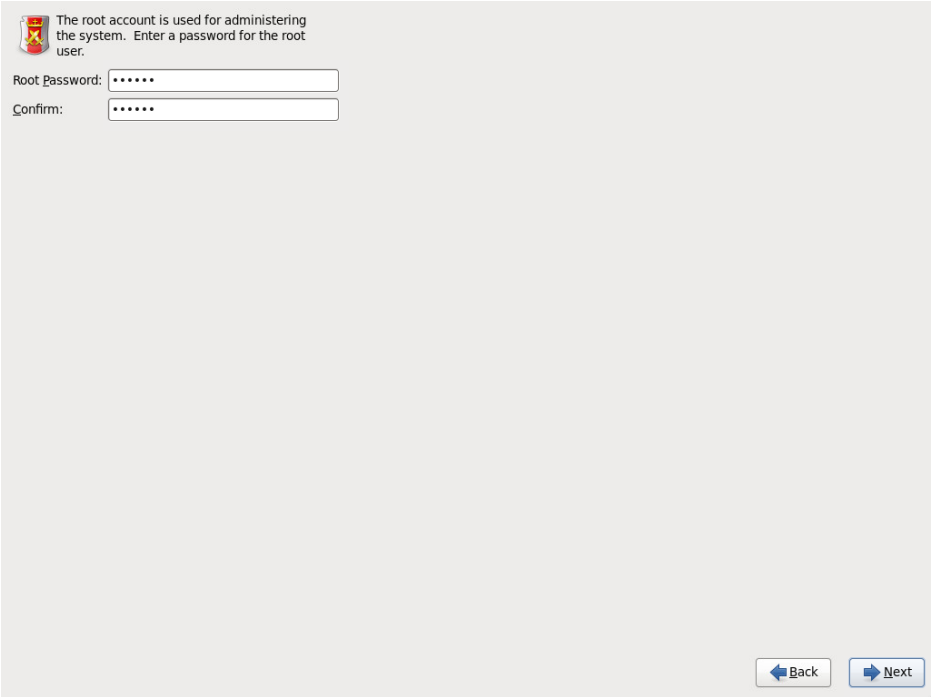
2.1.1.2. Timezone Specification



You can find your town in drop-down menu (sorting is being performed by one or other part of the World, for example, Moscow is included into Europe group) and, as well, on the map (use rolling lines and scale to navigate).

System clock uses UTC checkbox is being used when system uses Greenwich time (UTC).

2.1.1.3. System Superuser Password Creation



Root is system superuser. *Root* can't be used without password.

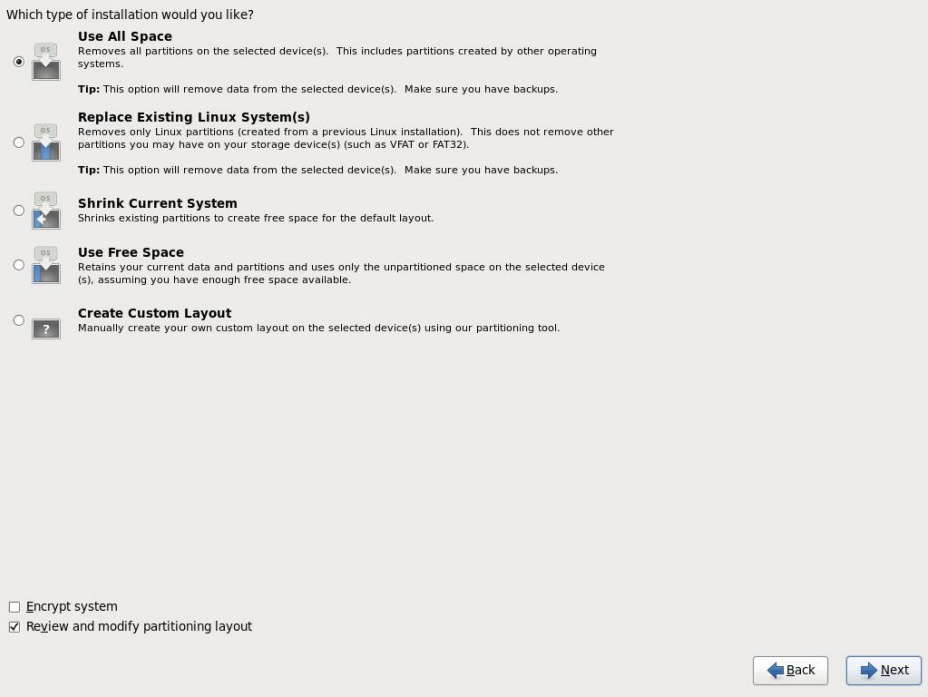
In case your password does not match requirements, you'll have a warning **Weak Password** window. Use the following buttons:

- **Use anyway** – when you want to create a password despite recommendations;
- **Cancel** – when you want to change the password.

> **Note:**
>
> Recommendations on password creation are available in chapter User name and password recommendation on page 59.

2.1.1.4. Choosing Disk Layout

> **Warning!**
>
> After the System was installed, the components will be located in the following directories:
>
> - InfoWatch Traffic Monitor – to `/opt/iw`;
> - Oracle DB – to `/u01` and `/u02`.
>
> If TM Server and Oracle DB are installed individually (see i. 2.1.2 on page 26 and i. 2.1.3 on page 37), then those directories will be located on different servers.

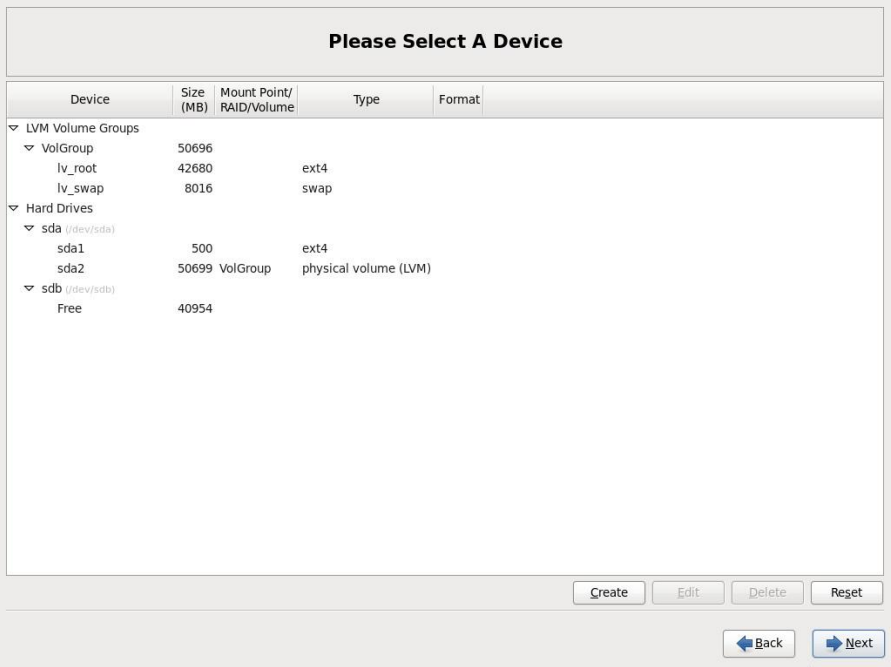


Use on of the disk layout types:

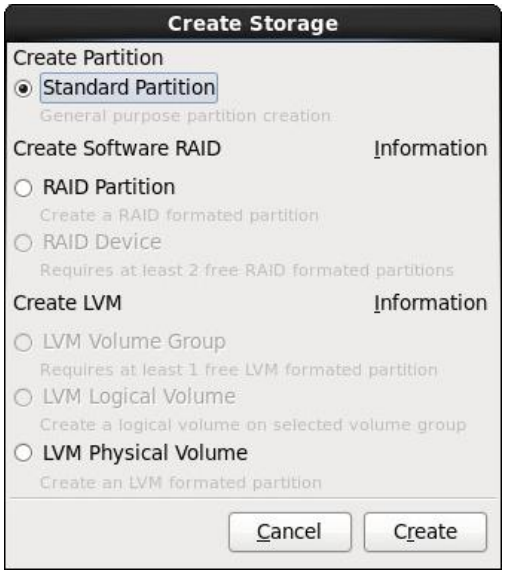
- **Use All Space** – all the partitions will be deleted, including those, which have been creation by other operating systems. All information on the chosen device will be destroyed, take care of the data backup;
- **Replace Existing Linux System(s)** – system volumes, created by previous OS Linux system, are being deleted. Other partition (for example, VFAT or FAT32), created on device (devices), will be saved. All information on the chosen device will be destroyed, take care of the data backup;
- **Shrink Current System** – existing partition will be compressed to release disk space;
- **Use Free Space** – keeps data and partitions: only unallocated space will be used;
- **Create Custom Layout** – creates custom partitioning on a device (devices).

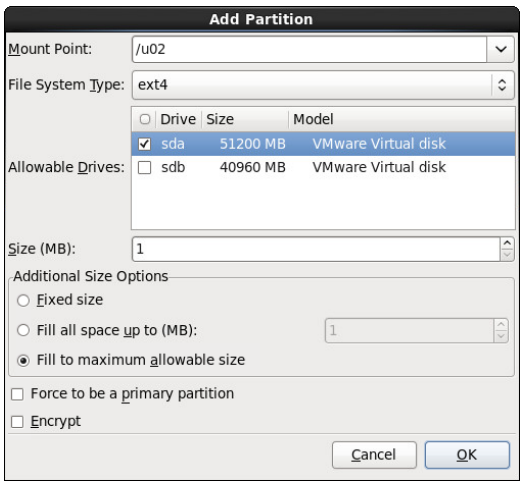
Additional settings:

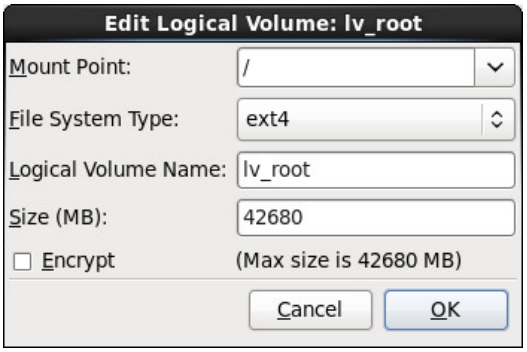
- **Encrypt system** – flag to encrypt system volumes.
- **Review and modify partitioning layout** – flag to review and modify partitioning layout.



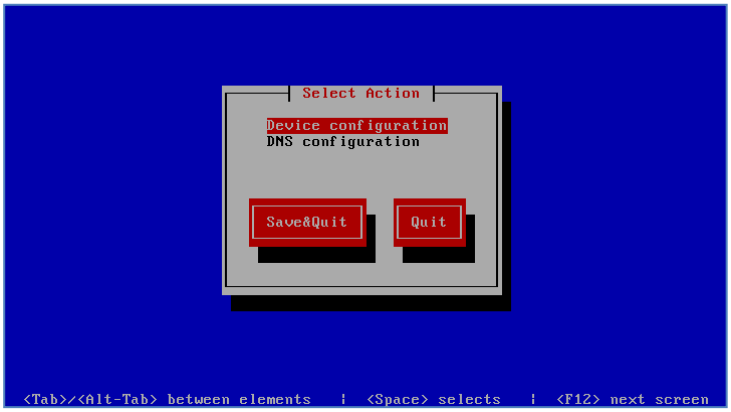
Here you can create, edit, delete or reset partition to its initial configuration.





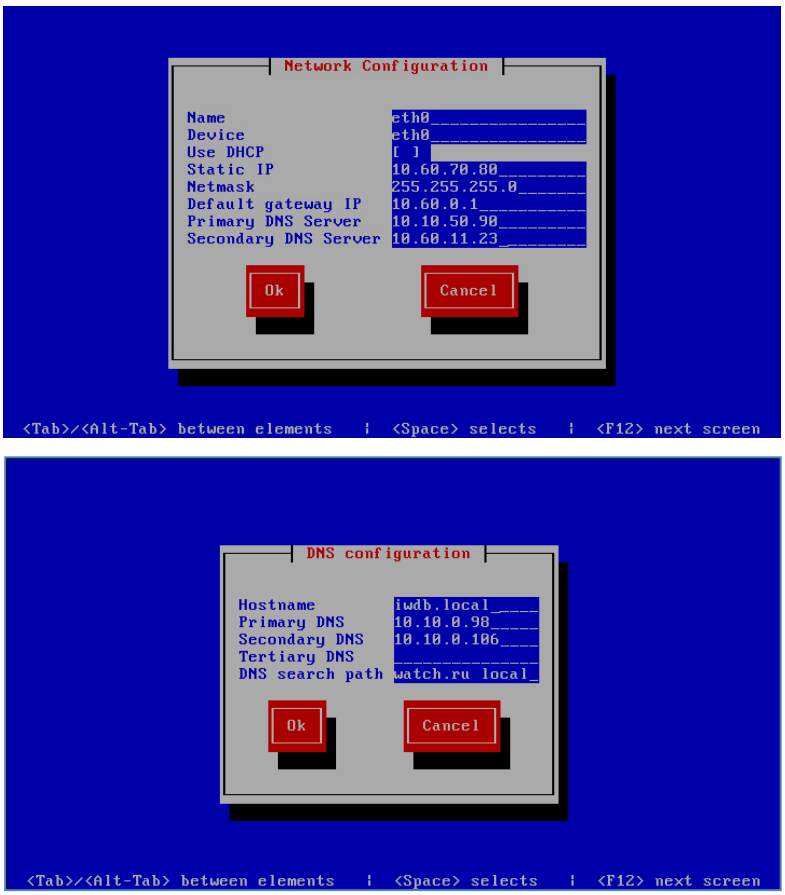


2.1.1.5. Network Settings



To set network card parameters, use (by pressing **Enter**):

- **Device configuration** – network card configuration.
- **DNS configuration** – DNS configuration.

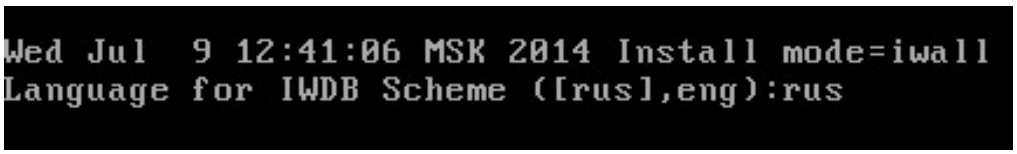


2.1.1.6. DB Language Choice

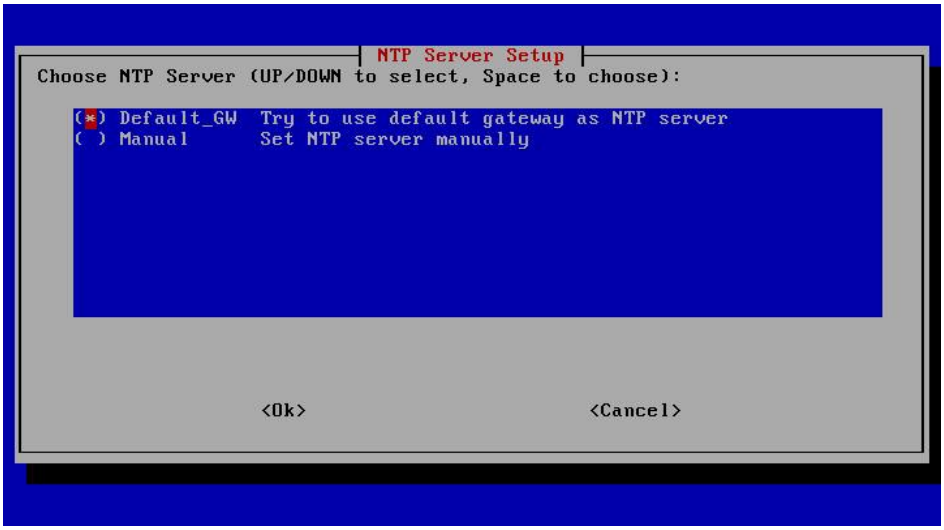
Choose one of two DB languages:

- *rus* – to install Russian DB;
- *eng* – to install English DB.

Language of classificatory, filters and default policies will have the chosen language.



2.1.1.7. Configuring Timezone Synchronization (NTP-Server)



DNS server is normally used in companies as time server (as domain controller).

Note:

In case you can't specify NTP-server, press **Cancel** and make this setting later (find detailed information on NTP-server in «*InfoWatch Traffic Monitor. Administration guide*»).

2.1.1.8. Installation Completion

The following accounts will be created:

Account	Name	Password
Linux Superuser´s account (root)	root	xxXX1234
Oracle Administrator	sys	xxXX1234
	system	xxXX1234
Oracle: Database Schema Owner	iwtm	xxXX1234
Oracle: a Linux user of DBMS, whose account will be used to load intercepted objects into the database	iwtm_linux	xxXX1234
Management Web-Console: User Administrator	administrator	xxXX1234
Management Web-Console: Security Officer	officer	xxXX1234
Linux user for launching Oracle server procedures	oracle	xxXX1234
Linux user for launching Traffic Monitor server procedures	iwtm	No password
Oracle DBMS client installation´s owner group including iwtm and oracle users	oinstall	-

> **Warning!**
>
> Please change passwords for root and oracle account immediately after installation is completed.

Server will receive the hostname as follows:

```
iwdb-xxxxxxxxxxxxxxxx.local
```

where:

- xxxxxxxxxxxxxxxx is a Serial Number of a server.

2.1.2. Installation from TME Package

Depending on server purpose (Traffic Monitor server or Database server or both components installed on a single computer), the set of installed components will be different:

Installation mode	Kickstart key	Order of components installation and configuration
"All-in-one" mode: all components are installed to a single server.	**IWALLX**	• Installing OS Linux • Configuring network interface • Installing and configuring Oracle DBMS • Installing IW Traffic Monitor database schema • Installing RPM packages of IWTM server

		• Installing Monitoring subsystem
Installing TM Appliance	**IWTMAX**	**Warning!** This type of installation is described in «InfoWatch Traffic Monitor Appliance. Installation guide»
Installing the Oracle DBMS Server with a Traffic Monitor database schema to a separate computer	**IWDBX**	• Installing OS Linux • Configuring network interface • Installing and configuring Oracle DBMS • Installing IW Traffic Monitor database schema • Installing Monitoring subsystem
Installing the Traffic Monitor Server to a separate computer	**IWTMX**	• Installing OS Linux • Configuring network interface • Installing RPM packages of IWTM server • Installing Monitoring subsystem

Guide for each installation type:

- "All-in-one" Installation Mode (IWALLX) (see i. 2.1.2.1 on page. 27);
- Database Installation (IWDBX) (see i. 2.1.2.2 on page 33);
- Traffic Monitor server installation (IWTMX) (see i. 2.1.2.3 on page 35);

2.1.2.1. "All-in-one" Installation Mode (IWALLX)

"All-in-one" installation mode allows installing the System on one computer.

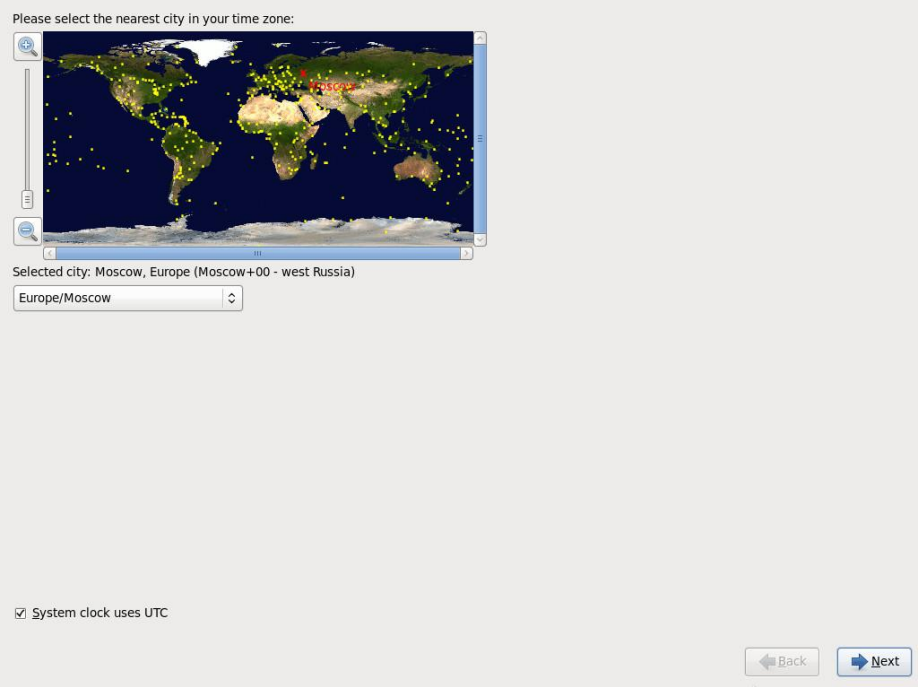
> **Warning!**
>
> This chapter contains guidance without detailed description of installation screens. Find additional information in chapter «Major information about installation steps» (see i. 2.1.1 on page 19).

To install «All-in-one», follow the steps below:

1. In **kickstart** window choose **IWALLX**, press **Enter**.

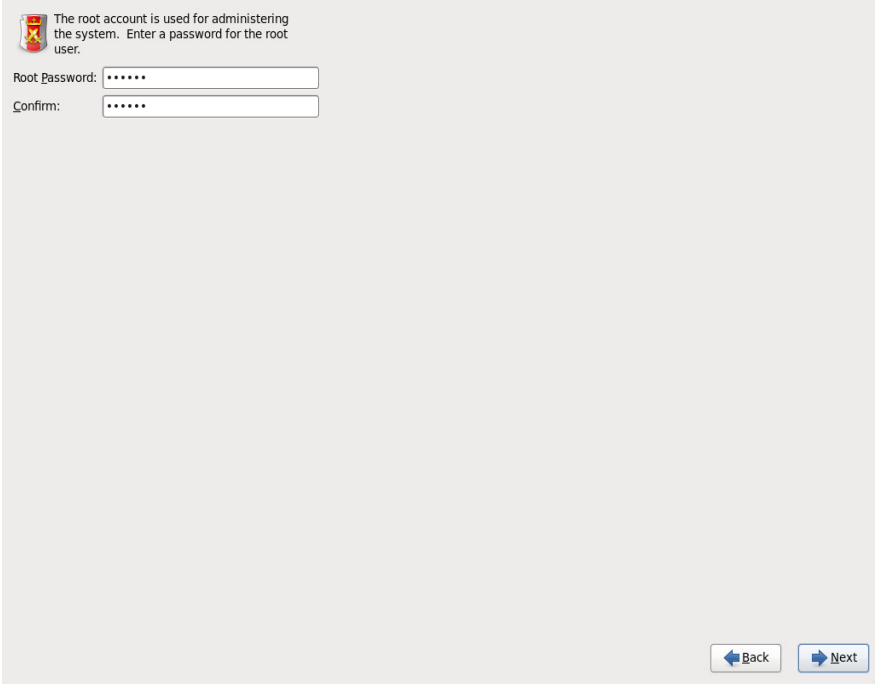
> **Warning!**
>
> You can see a warning when installation type has been chosen: «*The storage device below may contain any data*». To clean up the drive and start installation, press **Yes, discard any data**, leaving **Apply my choice to all devices with undetected partitions of filesystems** with no changes.

2. Specify server time zone (in case system clock is set to Greenwich (UTC), flag **System clock uses UTC** checkbox), press **Next**.



Select the time zone

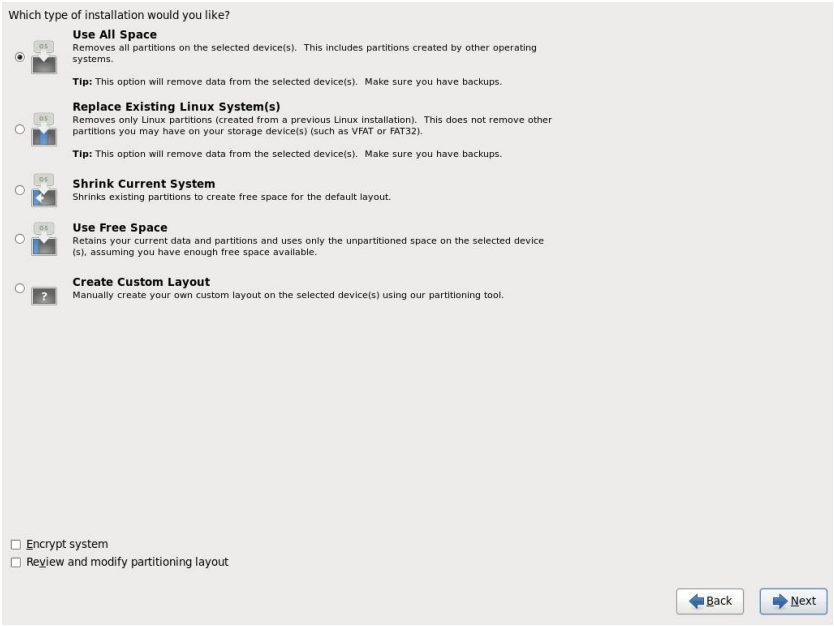
3. Create *root* password, press **Next**.



Note:

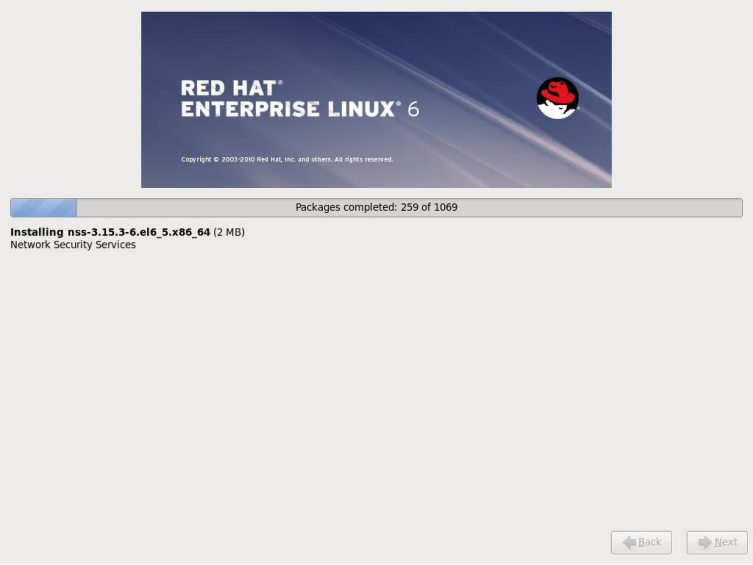
Find password recommendations in User name and password recommendation on page 59.

4. Specify disk layout :
   a) choose **Use All Space**;
   b) press **Next**.



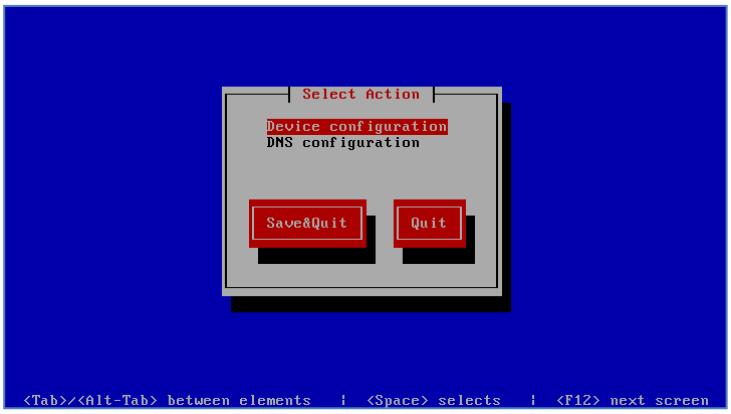
> **Note:**
>
> You could see **Format Warnings** on the screen, which indicate necessity of disk formatting before installation. To proceed with installation, press **Format**.

Disk partitioning will be started, and then – OS installation. You can see progress bar for both processes on the screen:

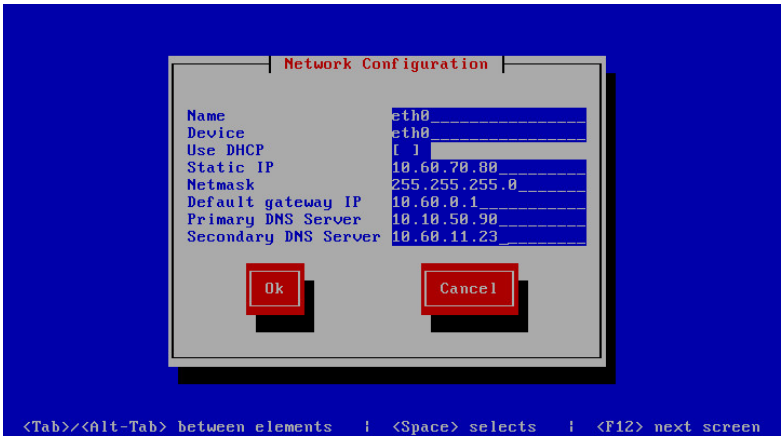


Process might take some time.

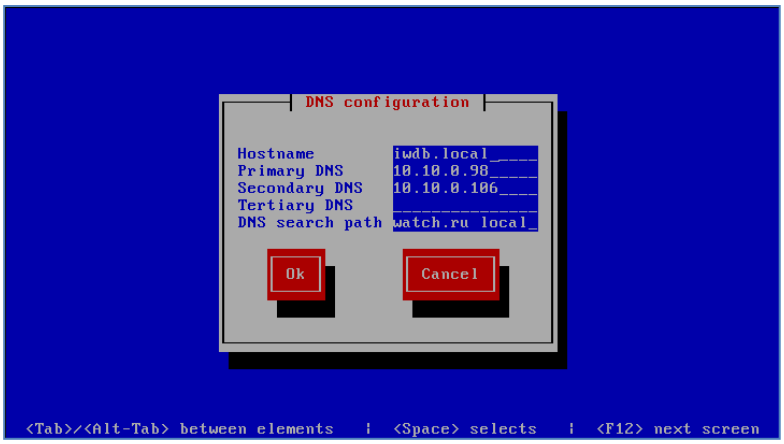
After OS installation, system will restart and you will see network configuration screen:



5. For network card parameters configuration:
   - Choose **Device configuration**, press **Enter**.
   - Choose **eth0** network interface, press **Enter**.
   - Move the cursor to **Use DHCP** field and press **Space**, specify server network configuration settings (static IP-address, etc.). Upon completion, press **OK**.
   - Press **Save** to save the settings.

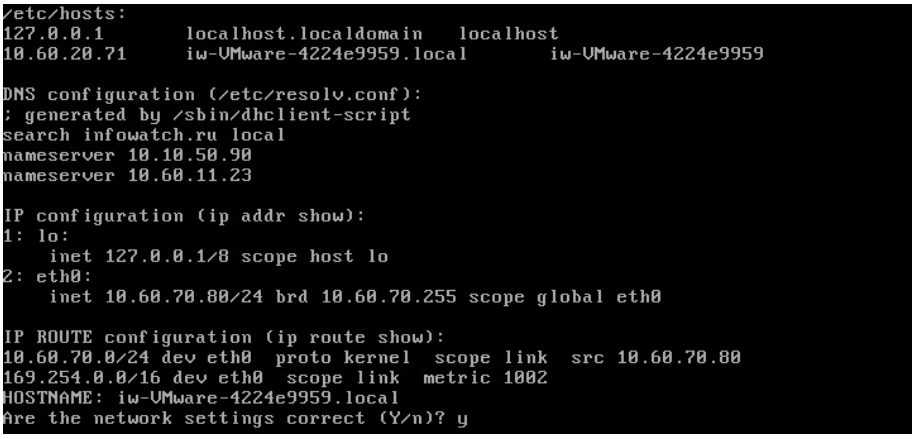


6. To configure DNS, choose **DNS configuration** and specify server network parameters. Press **OK**.



7. Press **Save&Quit**.

8. Verify specified system settings. When settings are incorrect, type in **N** and specify correct parameters (see steps 5 - 7). When settings are correct, type in **Y** to confirm and press **Enter**.

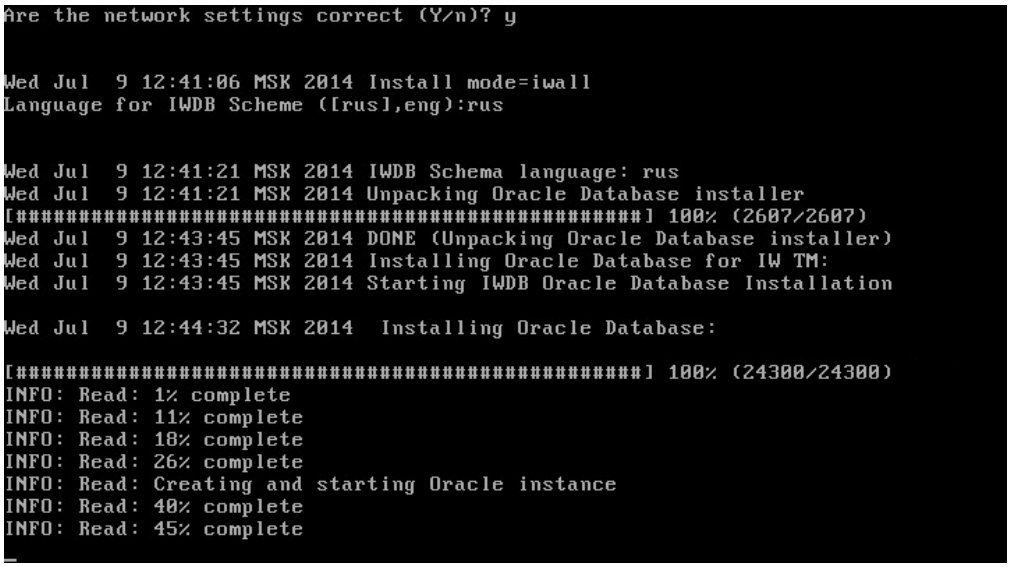


9. Specify DB schema language:
   - *rus* – to install Russian DB;
   - *eng* – to install English DB.

   Classifier, filters and default policies will be of the chosen language.

10. Press **Enter**.

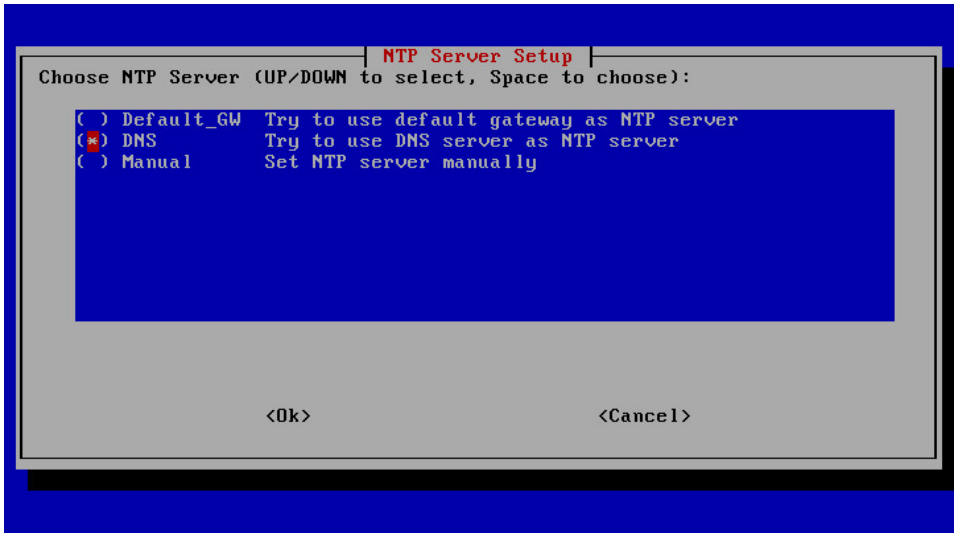
    Installation of Oracle DBMS and DB schema will start. You can track the progress on the screen:



    Process may take some time.

    Upon OS installation completion, reboot will be performed, you will need to specify server address for time synchronization (NTP-server).

11. Specify server address for time synchronization (NTP-server).



Normally DNS server is used as time server (as domain controller).

> **Note:**
>
> In case you can't specify NTP-server, press **Cancel** and make this setting later (find detailed information on NTP-server in «*InfoWatch Traffic Monitor. Administration guide*»)

As a result the following accounts will be created in the system:

Account	Name	Password
Linux Superuser´s account (root)	root	Set during installation
Oracle Administrator	sys	xxXX1234
	system	xxXX1234
Oracle: Database Schema Owner	iwtm	xxXX1234
Oracle: a Linux user of DBMS, whose account will be used to load intercepted objects into the database	iwtm_linux	xxXX1234
Oracle: user, which will be used for interaction between web-interface and Database	iwtm_web	xxXX1234
Management Web-Console: User Administrator	administrator	xxXX1234
Management Web-Console: Security Officer	officer	xxXX1234
Linux user for launching Oracle server procedures	oracle	`xxXX1234`
Linux user for launching Traffic Monitor server procedures	iwtm	No password
Oracle DBMS client installation´s owner group including `iwtm` and `oracle` users	oinstall	–

> **Warning!**
>
> Please change the password for `oracle` account immediately after installation is completed.

Server will receive the hostname as follows:

```
iwdb-xxxxxxxxxxxxxxx.local
```

where:

- xxxxxxxxxxxxxxx is a Serial Number of a server

Find system configuration procedure find in «*InfoWatch Traffic Monitor. Administration guide*»

2.1.2.2. Database Installation (IWDBX)

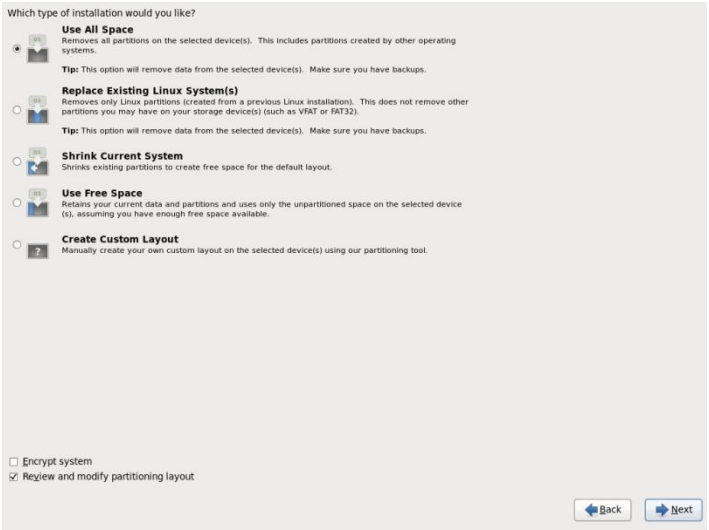
> **Warning!**
>
> This chapter contains guidance without detailed description of installation screens. Find additional information in chapter «Major information about installation steps» (see i. 2.1.1 on page 19).

To install database, follow steps below:

1. In **kickstart** window choose **IWDBX**, press **Enter**.

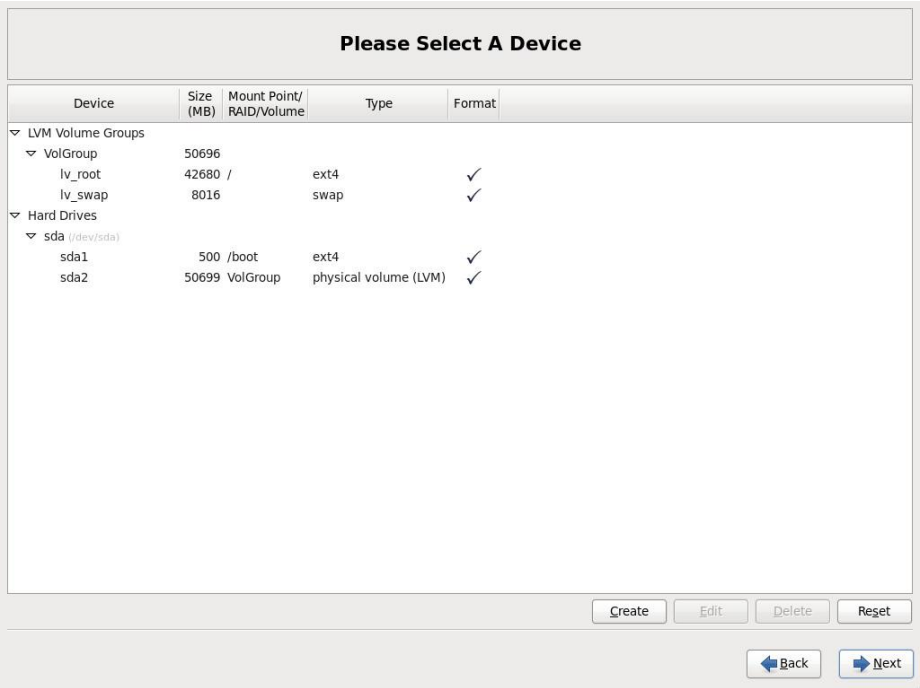
   > **Warning!**
   >
   > You can see a warming when installation type has been chosen: «*The storage device below may contain any data*». To clean up the drive and start installation, press **Yes, discard any data**, leaving **Apply my choice to all devices with undetected partitions of filesystems** with no changes.

2. Using description for **IWALLX** installation type, specify (i. 2.1.2.1, steps 2 and 3, respectively):
   - Server time zone;
   - *Root* password.
3. Specify disk layout:
   a) choose **Use All Space**;
   b) flag **Review and modify partitioning layout** checkbox.
   c) press **Next**.

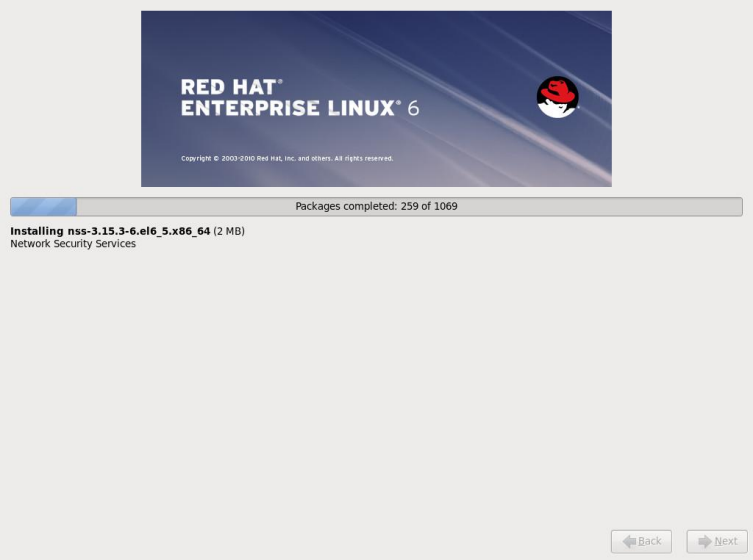


4. Perform disk partitioning, press **Next**.

> **Note:**
>
> Normally the following attributes are used:
>
> - **Mount Point** – value /;
> - **File System Type** – value `ext4`;
> - **Logical Volume Name** – value `lv_root`;
> - **Size (MB)** – default value (100 GB and more recommended);
> - **Encrypt** – default value.

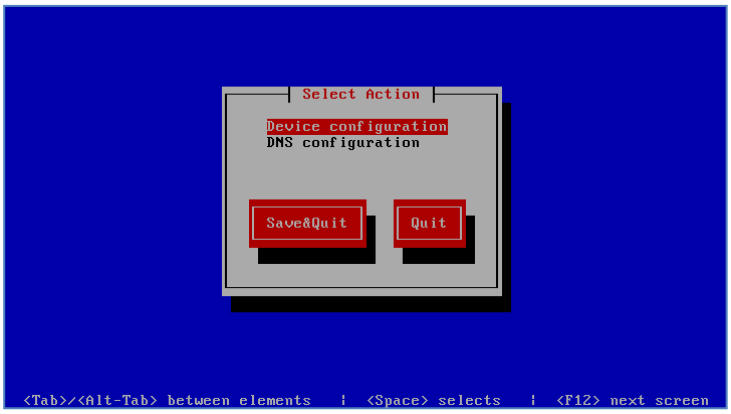


Disk partitioning will be started, and then – OS installation. You can see progress bar for both processes on the screen:



Process might take some time.

After OS installation, system will restart and you will see network configuration screen:



5. Using description for **IWALLX** installation type, make the rest of the settings (i. 2.1.2.1, steps 5 - 11).

2.1.2.3. Traffic Monitor server installation (IWTMX)

> **Warning!**
>
> This chapter contains guidance without detailed description of installation screens. Find additional information in chapter «Major information about installation steps» (see i. 2.1.1 on page 19).

To install Traffic Monitor server, follow steps below:

1. In **kickstart** window choose **IWTMX**, press **Enter**.

> **Warning!**
>
> You can see a warning when installation type has been chosen: «*The storage device below may contain any data*». To clean up the drive and start installation, press **Yes, discard any data**, leaving **Apply my choice to all devices with undetected partitions of filesystems** with no changes.

2. Using description for **IWALLX** installation type, specify (i. 2.1.2.1, steps 2 - 8, respectively):
   - Server time zone;
   - *Root password*;
   - Disk layout;
   - Network card parameters configuration;
   - DNS configuration settings;
3. Specify BD server IP-address, press **Enter**.

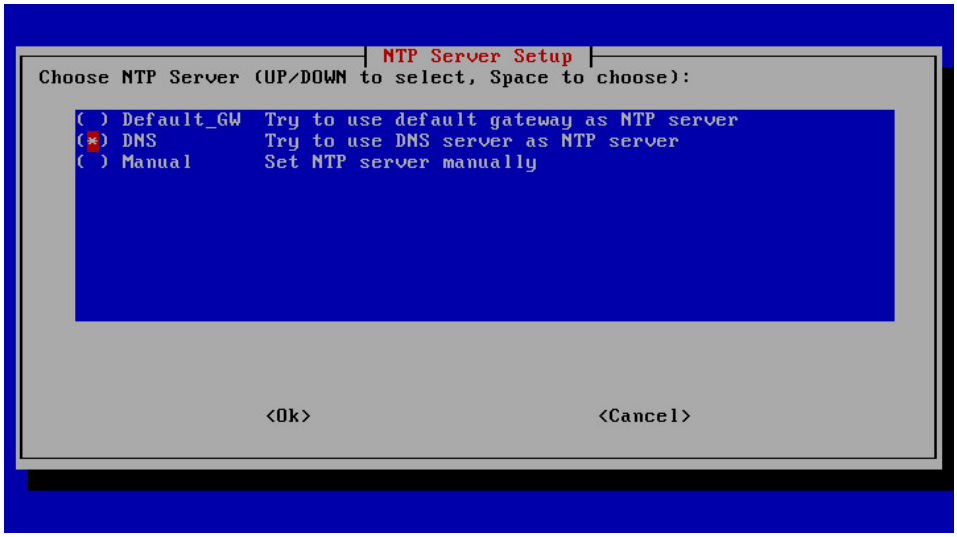
```
Complete!
Tue Nov 11 14:22:37 MSK 2014 Oracle Client Setup:
Enter IWDB ip address: _
```

4. Verify specified network settings. When settings are incorrect, type in **N** and specify correct parameters (see step 3). When settings are correct, type in **Y** to confirm and press **Enter**

```
Complete!
Tue Nov 11 14:22:37 MSK 2014 Oracle Client Setup:
Enter IWDB ip address: 10.60.21.32
IWDB ip address has been set to: 10.60.21.32
Is IWDB ip address correct (y/n)? y_
```

Upon OS installation completion, reboot will be performed, you will need to specify server address for time synchronization (NTP-server).

12. Specify server address for time synchronization (NTP-server).



Normally DNS server is used as time server (as domain controller).

> **Note:**
>
> In case you can't specify NTP-server, press **Cancel** and make this setting later (find detailed information on NTP-server in «*InfoWatch Traffic Monitor. Administration guide*»)

As a result the following accounts will be created in the system:

Account	Name	Password
Linux Superuser´s account (root)	root	Set during installation
Oracle Administrator	sys	xxXX1234
	system	xxXX1234
Oracle: Database Schema Owner	iwtm	xxXX1234
Oracle: a Linux user of DBMS, whose account will be used to load intercepted objects into the database	iwtm_linux	xxXX1234
Oracle: user, which will be used for interaction between web-interface and Database	iwtm_web	xxXX1234
Management Web-Console: User Administrator	administrator	xxXX1234
Management Web-Console: Security Officer	officer	xxXX1234
Linux user for launching Oracle server procedures	oracle	`xxXX1234`
Linux user for launching Traffic Monitor server procedures	iwtm	No password
Oracle DBMS client installation´s owner group including `iwtm` and `oracle` users	oinstall	–

> **Warning!**
>
> Please change password for `oracle` account immediately as the installation is completed.

Server will receive the hostname as follows:

```
iwdb-xxxxxxxxxxxxxxxx.local
```

where:

- xxxxxxxxxxxxxxxx is a Serial Number of a server.

2.1.3. Installation from TMS Package

The table contains different installation types:

Installation mode	Kickstart key	Order of components installation and configuration
"All-in-one" mode: all components are installed to a single server.	**IWALLX**	• Installing OS Linux • Configuring network interface • Installing and configuring Oracle DBMS • Installing IW Traffic Monitor database schema • Installing RPM packages of IWTM server • Installing Monitoring subsystem
Installing TM Appliance	**IWTMSX**	**Warning!** This type of installation is described in «InfoWatch Traffic Monitor Appliance. Installation Guide»

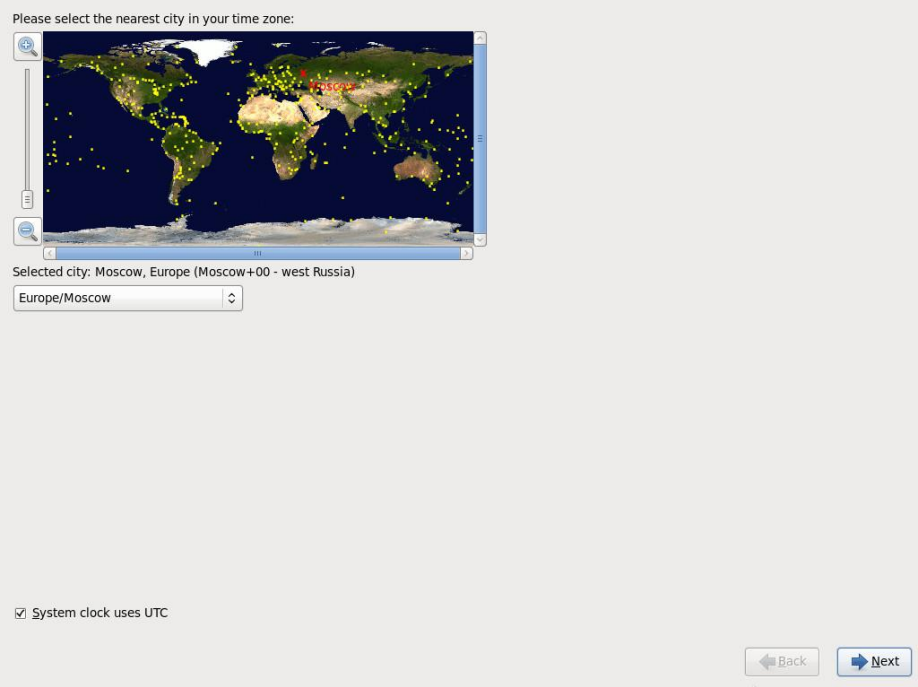
> **Warning!**
>
> This chapter contains guidance without detailed description of installation screens. Find additional information in chapter «Major information about installation steps» (see i. 2.1.1 on page 19).

To install «All-in-one», follow the steps below:

1. In **kickstart** window choose **IWALLX**, press **Enter**.

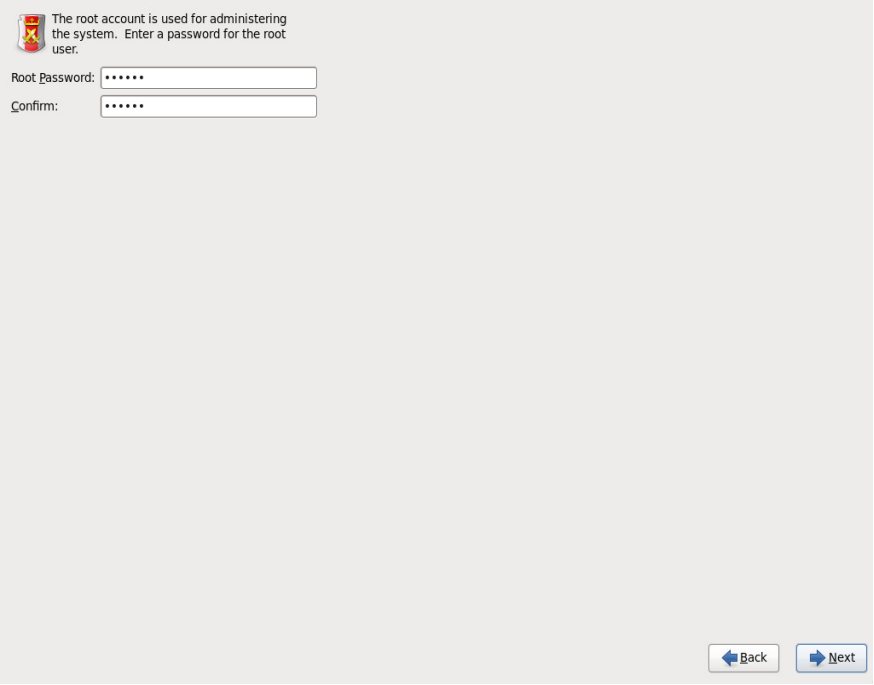
> **Warning!**
>
> You can see a warning when installation type has been chosen: «*The storage device below may contain any data*». To clean up the drive and start installation, press **Yes, discard any data**, leaving **Apply my choice to all devices with undetected partitions of filesystems** with no changes.

2. Specify time zone settings for server (in case system time is set to Greenwich (UTC), flag **System clock uses UTC** checkbox, press **Next**.



Select the time zone

3. Specify *root* password, press **Next**.



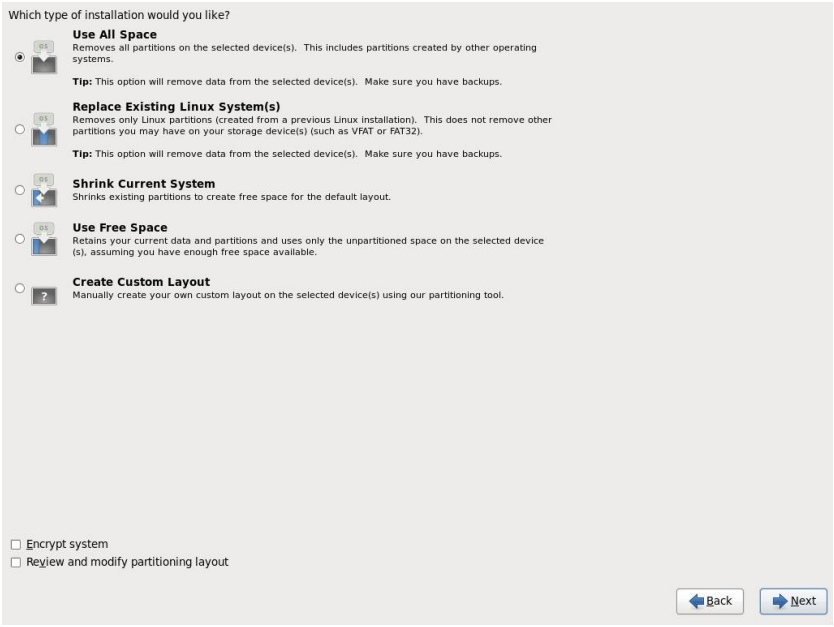
Note:

Find password recommendations in User name and password recommendation on page 59

4. Specify disk layout:

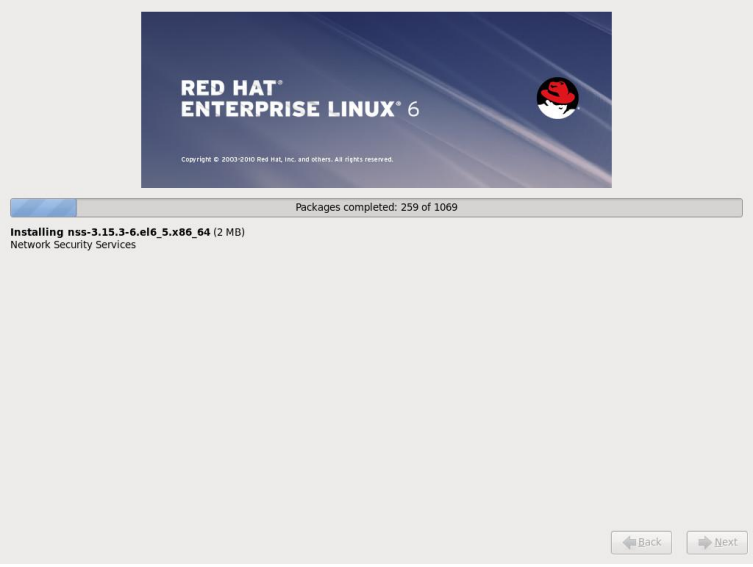
   c) choose **Use All Space**;

   d) press **Next**.



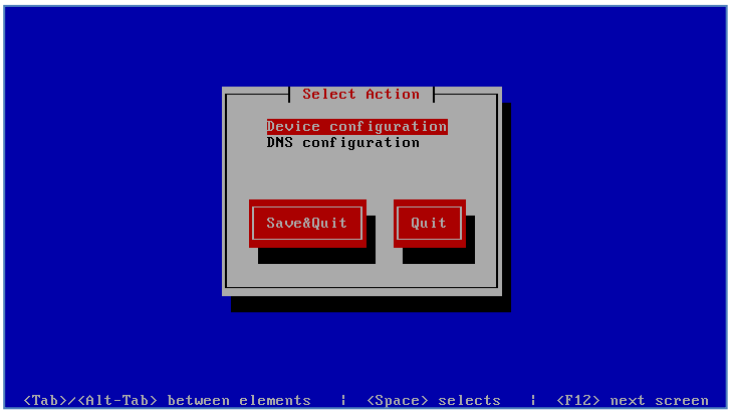
> **Note:**
>
> You could see **Format Warnings** on the screen, which indicate necessity of disk formatting before installation. To proceed with installation, press **Format**.

Disk partitioning will be started, and then – OS installation. You can see progress bar for both processes on the screen:

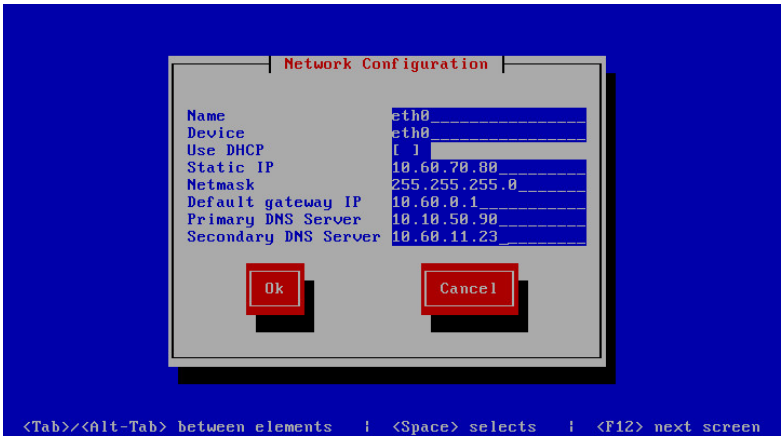


Process might take some time.

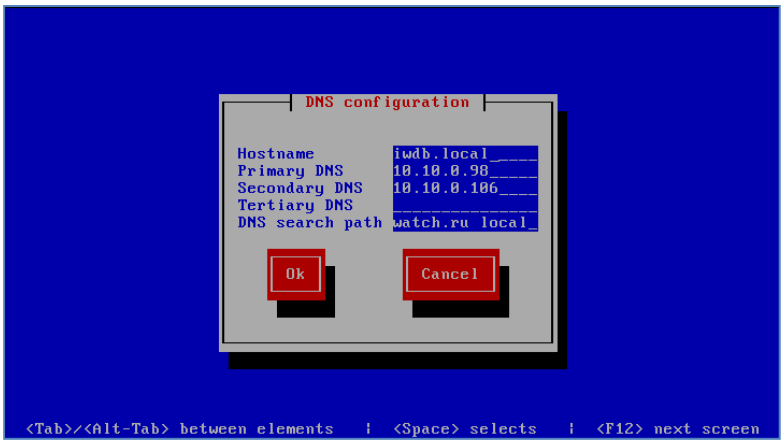
After OS installation, system will restart and you will see network configuration screen:



13. For network card parameters configuration:
    - Choose **Device configuration**, press **Enter**.
    - Choose **eth0** network interface, press **Enter**.
    - Move the cursor to **Use DHCP** field and press **Space**, specify server network configuration settings (static IP-address, etc.). Upon completion, press **OK**.
    - Press **Save** to save the settings.

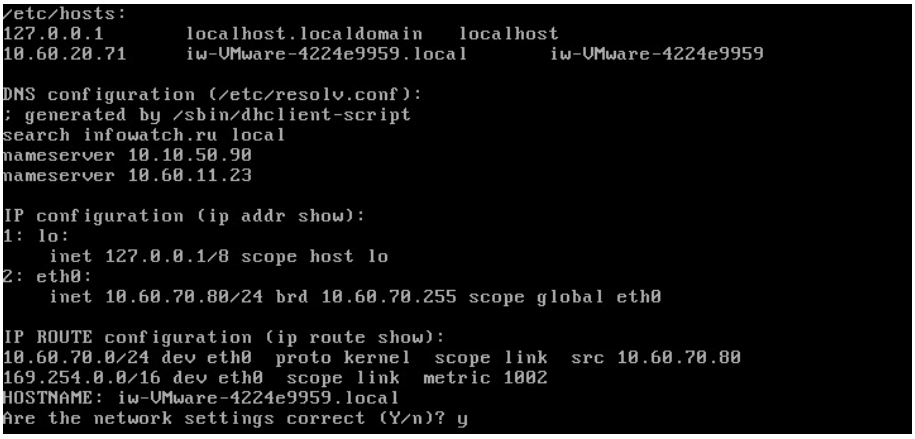


14. To configure DNS, choose **DNS configuration** and specify server network parameters. Press **OK**.



5. Press **Save&Quit**.

6. Verify specified system settings. When settings are incorrect, type in **N** and specify correct parameters (see steps 5 - 7). When settings are correct, type in **Y** to confirm and press **Enter**.



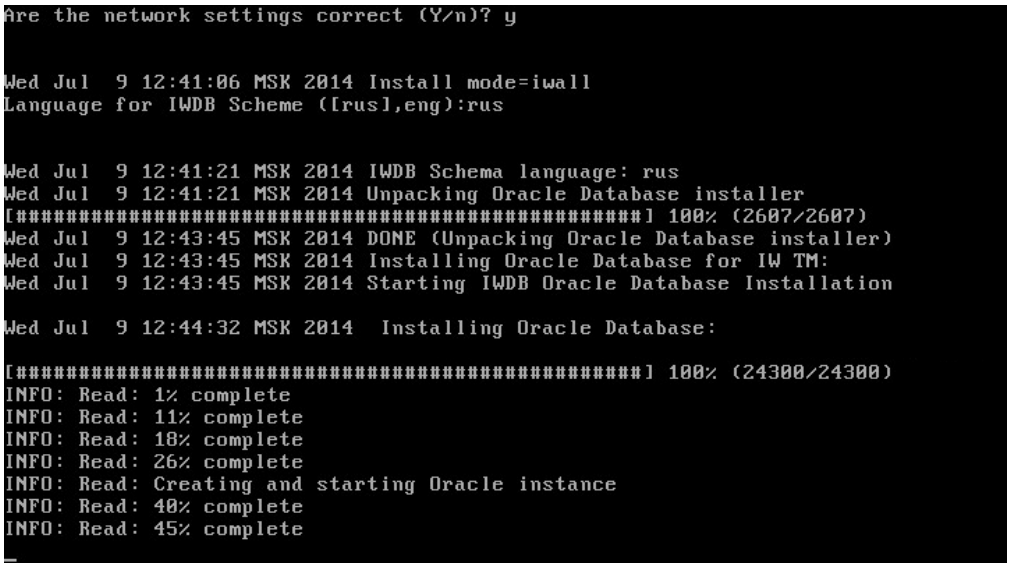
15. Specify DB schema language:

    - *rus* – to install Russian DB;
    - *eng* – to install English DB.

    Classifier, filters and default policies will be of the chosen language.

7. Press **Enter**.

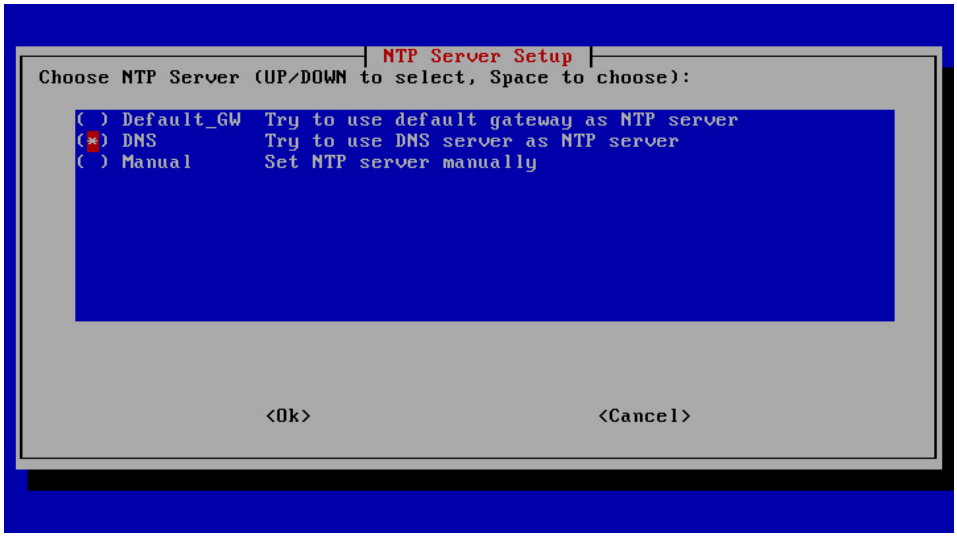
    Installation of Oracle DBMS and DB schema will start. You can track the progress on the screen:



    Process may take some time.

    Upon OS installation completion, reboot will be performed; you will need to specify server address for time synchronization (NTP-server).

8. Specify server address for time synchronization (NTP-server).



Normally DNS server is used as time server (as domain controller).

> **Note:**
>
> In case you can't specify NTP-server, press **Cancel** and make this setting later (find detailed information on NTP-server in «*InfoWatch Traffic Monitor. Administration guide*»).

As a result the following accounts will be created in the system:

Account	Name	Password
Linux Superuser´s account (root)	root	Set during installation
Oracle Administrator	sys	xxXX1234
	system	xxXX1234
Oracle: Database Schema Owner	iwtm	xxXX1234
Oracle: a Linux user of DBMS, whose account will be used to load intercepted objects into the database	iwtm_linux	xxXX1234
Oracle: user, which will be used for interaction between web-interface and Database	iwtm_web	xxXX1234
Management Web-Console: User Administrator	administrator	xxXX1234
Management Web-Console: Security Officer	officer	xxXX1234
Linux user for launching Oracle server procedures	oracle	`xxXX1234`
Linux user for launching Traffic Monitor server procedures	iwtm	No password
Oracle DBMS client installation´s owner group including `iwtm` and `oracle` users	oinstall	–

> **Warning!**
>
> Please change password for `oracle` account immediately as the installation is completed.

Server will receive the hostname as follows:

```
iwdb-xxxxxxxxxxxxxxx.local
```

where:

- xxxxxxxxxxxxxxx is a Serial Number of a server.

For system configuration, see «*InfoWatch Traffic Monitor. Administration Guide*»

2.2. Web-Console Installation

Web-console installation is being performed in automatic mode by means of **kickstart** installation program. As server components have been installed (see i. Server Components Installation on page 18), web-console becomes available via browser window, wherein you need to specify local DB server URL-address.

2.3. Crawler Subsystem Installation

The Crawler interceptor is designed as two Windows services:

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

> **Warning!**
>
> One DB Traffic Monitor can be used by **only one** Crawler server instance. One Crawler server can support **only one** Crawler scanner instance.

For all Crawler components installation (server and scanner) the same distributive is used.

> **Warning!**
>
> Both Crawler server and Crawler scanner should be installed to computers located in the same domain: the one to which all workstations to scan are belong.

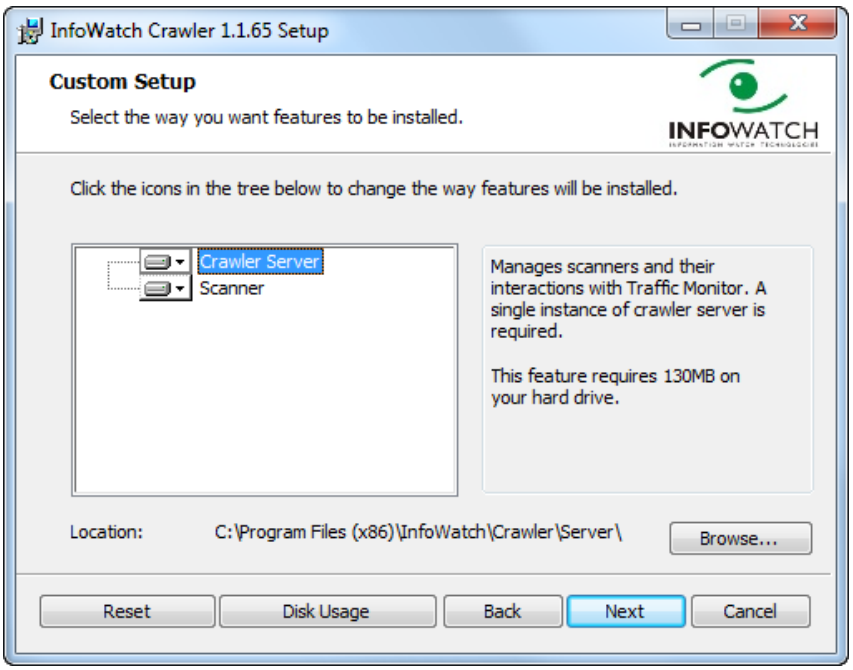
For hardware and software requirements to computers where Crawler components will be installed see i. 1.2.6 on page 15.

To install the Crawler:

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

   > **Note:**
   >
   > The installation language is defined automatically and depends of chosen format (see **Start -> Control Panel -> Region and Language**, **Formats** tab).

2. At the InfoWatch Crawler welcome screen click **Next**.
3. At the **Installation Scope** screen click **Next**.
4. At the **Custom Setup** screen select which Crawler components should be installed and where to:
   - **Crawler Server** – installing the `InfoWatch.Crawler.Server` service managing scanning tasks and provides communication with the server, database and Traffic Monitor Management Console.
   - **Scanner** – installing the `InfoWatch.Crawler.Scaner` service scanning network folders and file storages according to settings configured by user.

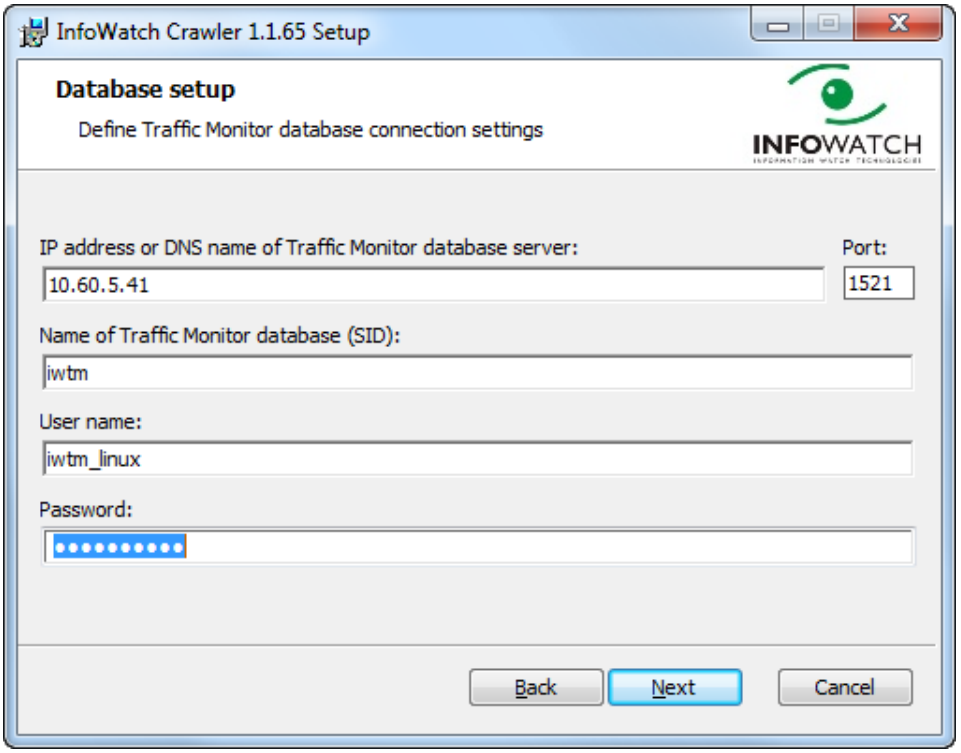


a) If you don't need any component, select it and click ✕ **Entire feature will be unavailable** in the drop-down menu.

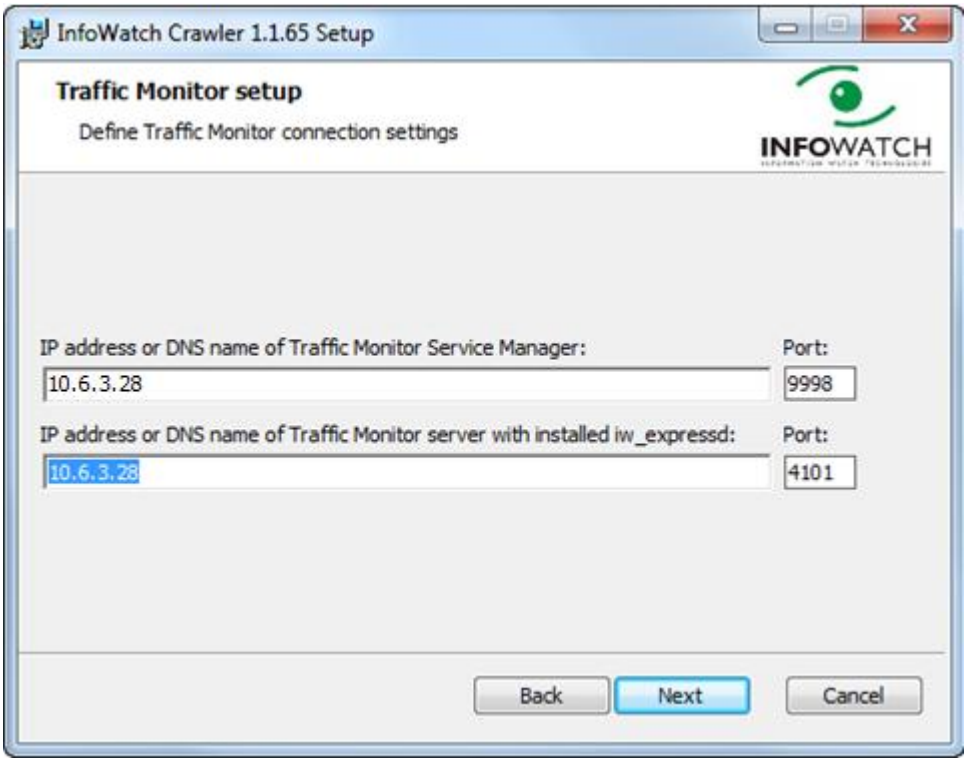
b) Specify path to directories where to components will be installed and click **Next**.

c) If at **Custom Setup** step you chose **Crawler Server** component:

1) Specify parameters of connecting the `InfoWatch.Crawler.Server` service with Traffic Monitor database, click **Next**.



2) Specify parameters of connecting the `InfoWatch.Crawler.Server` service with Traffic Monitor server, press **Next**.

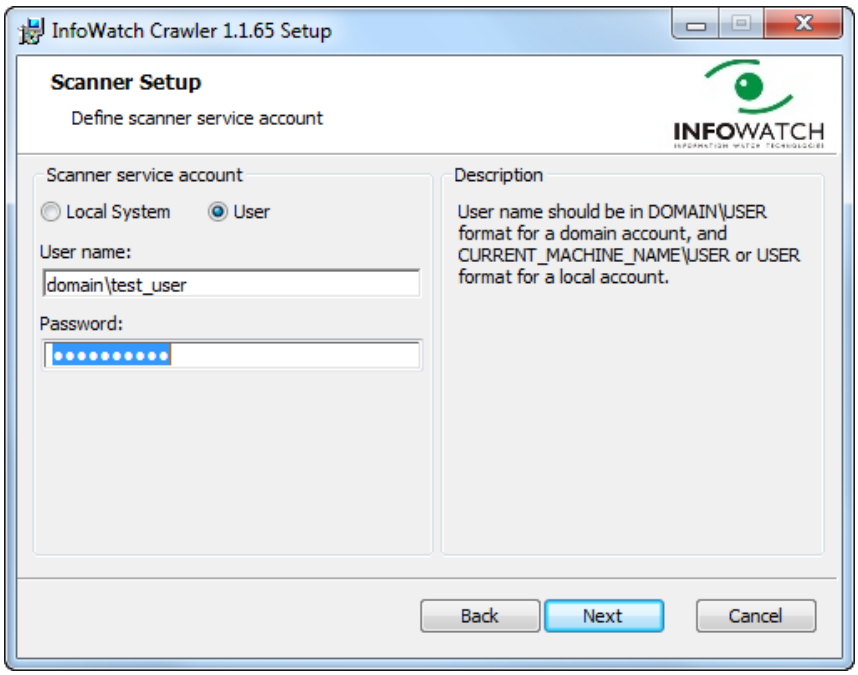


Warning!

User name should be the same as a name of Oracle account used for managing the Linux part of IWTM (`iw_adlibitum`, `iw_dbloader`, `iw_updater`). If you installed the system from the kickstart with default options, this is **iwtm_linux**.

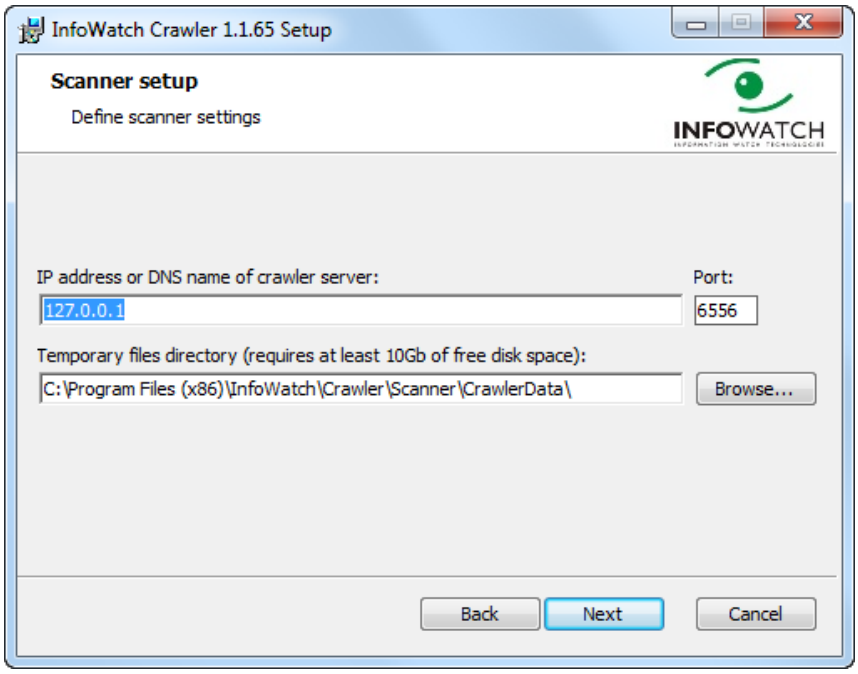
d) If at **Custom Setup** step you chose **Scanner** component:

1) Specify a name of account used for `InfoWatch.Crawler.Scaner` service running. You can select standard Local System account (recommended option) or enter parameters of an account having a rights for running services in the background (this option is configured in **Control Panel –> Administrative Tools –> Local Security Policy –> local policies –> User Rights Assignment –> log on as a service**). Click **Next**.



2) Specify:

- IP address or DNS name of the computer where the Server component is installed;
- Crawler server's port number;
- Link to the directory to where the scanner will temporary save files copied from reviewed resources.



5. Click **Next**.
6. Click **Install** to start Crawler installation. Follow the instructions to complete installation

2.4. Installing the InfoWatch Lync Adapter

In this chapter:

- Installing the InfoWatch Transfer Service 1.0 (i. 2.4.1 on page 48).
- Installing the IW OCS Filter 2.0 (i. 2.4.2 on page 50).

InfoWatch Lync Adapter contains of two modules: InfoWatch Transfer Service 1.0 and IW OCS Filter 2.0.

2.4.1. Installing the InfoWatch Transfer Service 1.0

InfoWatch Transfer Service 1.0 should be installed just before IW OCS Filter 2.0 installation. InfoWatch Transfer Service 1.0 is a service sending contexts intercepted by IW OCS Filter 2.0 to the IWTM.

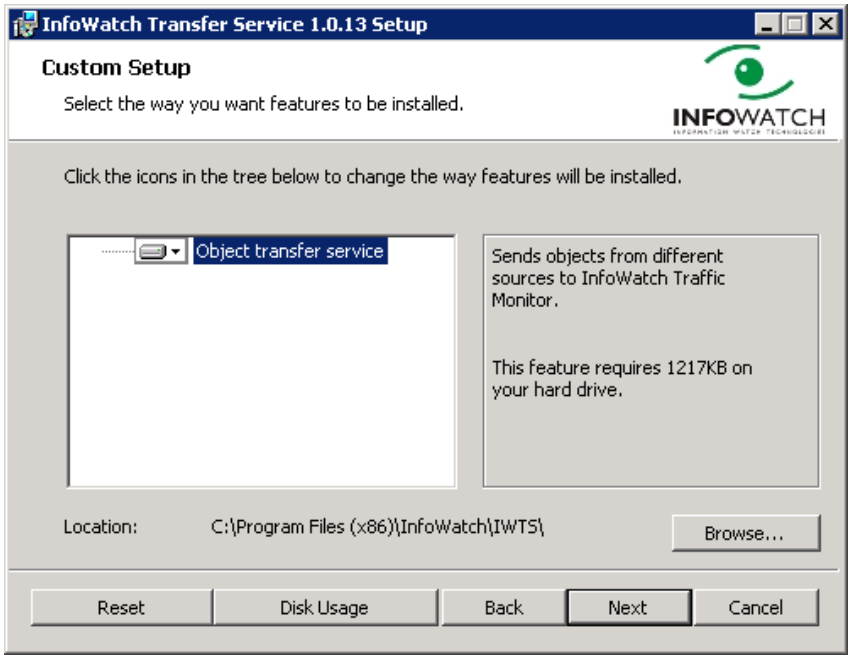
The installation is performed automatically by means of the installation package.

To install the InfoWatch Transfer Service:

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

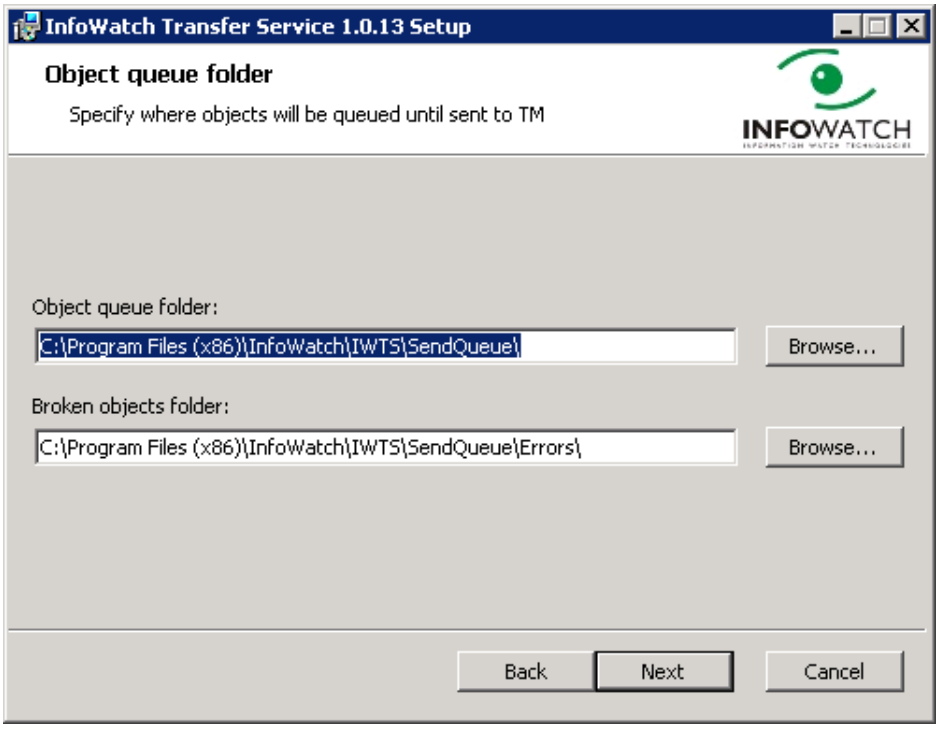
   > **Note:**
   >
   > The installation language is defined automatically and depends of chosen format (see **Start -> Control Panel -> Region and Language**, **Formats** tab).

2. At the InfoWatch Transfer Service welcome screen click **Next**.
3. At the **Installation Scope** screen click **Next**.
4. At the **Custom Setup** screen you can specify a path to the directory where the IWTS components will be installed to.



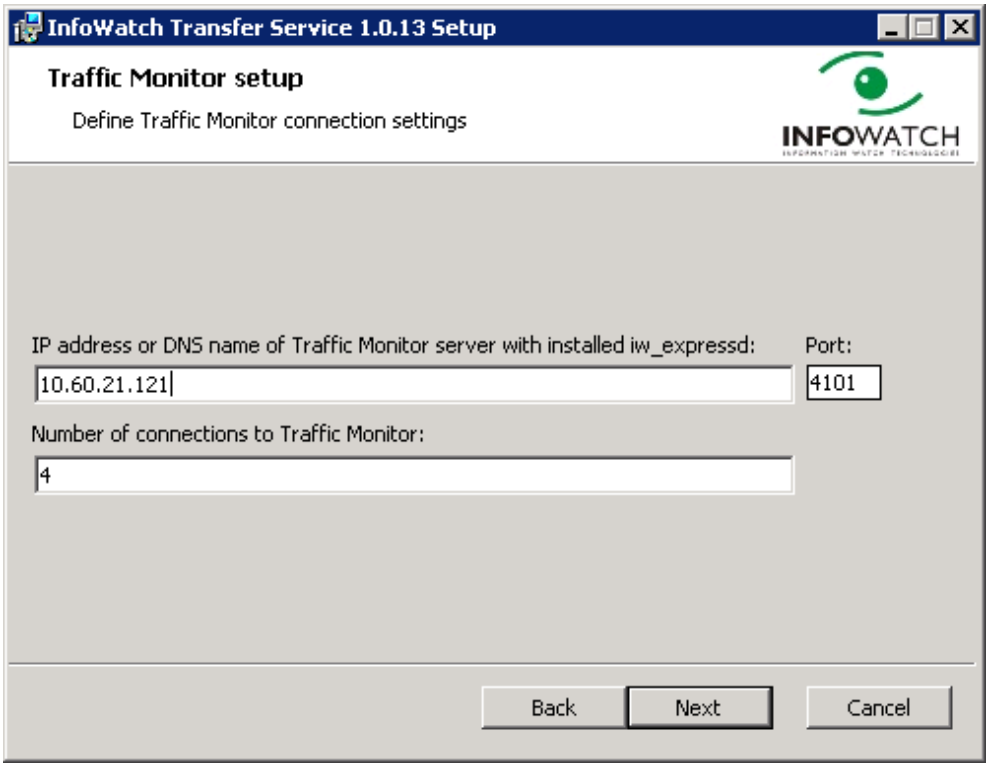
   Click **Next**.

5. Specify a path to the directory where the object queues will be stored:
   - **Object queue folder** is the directory for storing the contexts which IWTS sends to IWTM.
   - **Broken objects folder** is the directory for storing the contexts which attempt of sending to IWTM was ended with an error.



Click **Next**.

6. Specify parameters of connecting the IWTS service with Traffic Monitor server.
   - **IP address or DNS name of Traffic Monitor server with installed iw_expressed** – the address of the Traffic Monitor server.
   - **Number of connections to Traffic Monitor** – the number of simultaneous data transfer channels.



Click **Next**.

7. Click **Install** to start IWTS installation.
8. To complete installation click **Finish**.

2.4.2. Installing the IW OCS Filter 2.0

The installation is performed at the Microsoft Lync Server 2010/2013 server which is the front-end server (or Standard Edition server).

The installation is performed automatically by means of the installation package.

To perform the installation you should:

- Use an account having privileges of:
  - administrator of the domain where the Microsoft Lync Server 2010/2013 is deployed
  - local administrator of the server where the Microsoft Lync Server 2010/2013 is deployed.
- Create a local account of a user running the module service. This account should have rights of local administrator on the local computer and included to the `RTC Server Applications` group.

> **Note:**
>
> The account which (while installation) you will specify as used for IW OCS Filter service running, will automatically receive required rights for service running. Otherwise you should make appropriate changes in the local group policy.

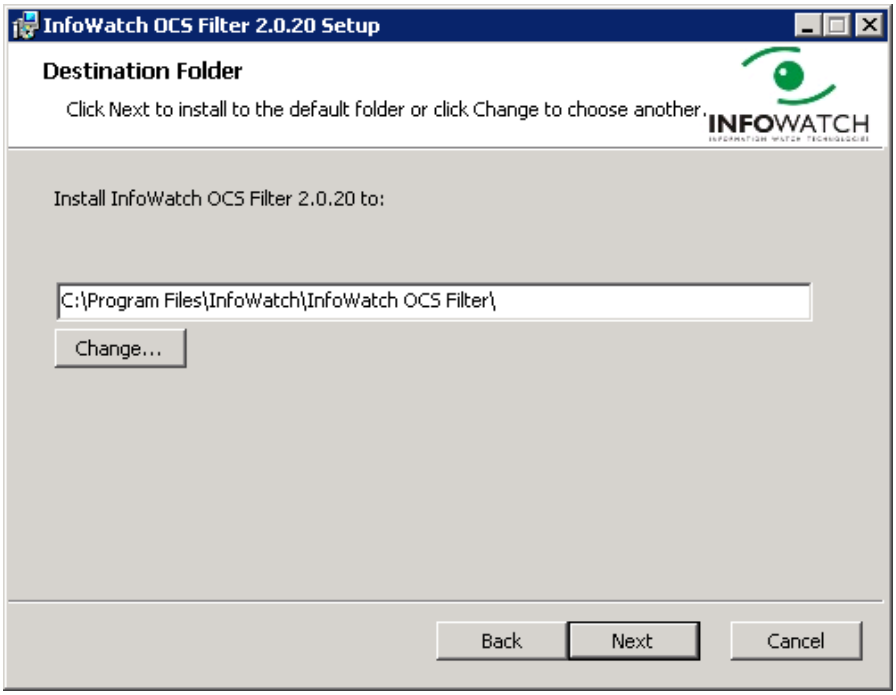
To install the InfoWatch OCS Filter:

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

   > **Note:**
   >
   > The installation language is defined automatically and depends of chosen format (see **Start -> Control Panel -> Region and Language**, **Formats** tab).

2. At the IW OCS Filter welcome screen click **Next**.

3. At the **Destination Folder** screen you can change a path to the directory where the IW OCS Filter components will be installed to.

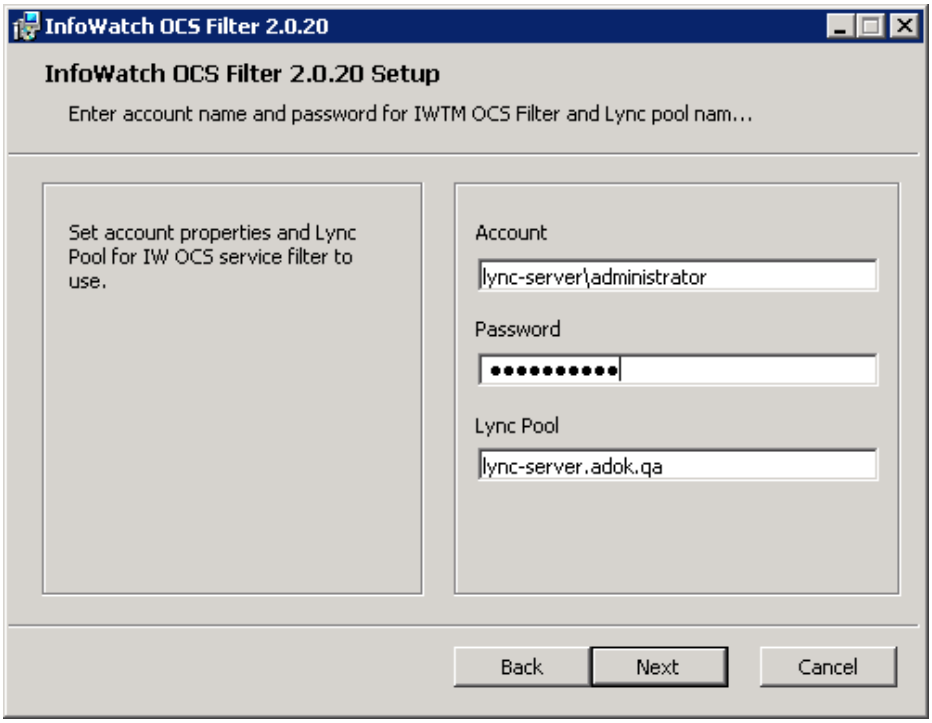


   Click **Next**.

4. Specify credentials needed for IW OCS Filter service running:
   - Username and password of account used for IW OCS Filter service running.

     > **Note:**
     >
     > Username should be specified as <computer>\<username> where <computer> is a name of server which will be the service installed to, and <username> is account name

   - The address of Microsoft Lync 2010/2013 pool which will be used for IW OCS Filter registering.



   Click **Next**.

5. Click **Install** to start IW OCS Filter installation.
6. To complete installation click **Finish**

For additional information on adapter configuration see «*InfoWatch Traffic Monitor. Administration Guide*».

CHAPTER 3. UPDATING THE SYSTEM

To update the System with IWALLX installation type:

1. Update RHEL and IWTM packages (see i. 3.1 on page 52)
2. Update DB scheme (see i. 3.2 on page 53)
3. Reboot the Server.

To update the System with IWTM+IWDBX installation type:

1. On TM and DB Servers update RHEL and IWTM (see i. 3.1 on page 52)
2. On DB Server update DB scheme (see i. 3.2 on page 53)
3. Reboot DB Server.
4. Reboot TM Server.

Before starting an update process, check, whether `/opt/iw/tm5/iwks_mode` file is present in the system. Installation type, mentioned in the file should match the actual installation type.

File might contain one of the following parameters:

Parameter	Meaning
`iwall`	All InfoWatch Traffic Monitor Enterprise components are being installed on one server
`iwtm`	Traffic Monitor Server is being installed on a separate computer
`iwdb`	Oracle DBMS with DB scheme is being installed on a separate computer
`iwtms`	All InfoWatch Traffic Monitor Standard components are being installed on one server
`apple`	InfoWatch Traffic Monitor Appliance Enterprise
`appls`	InfoWatch Traffic Monitor Appliance Standard

3.1. Updating RHEL and IWTM packages

To update the System, one needs to connect **kickstart** disk first. Packages, required for update, are being installed from the mentioned disk.

1. In a random hard drive partition, create a directory and mount CD-disk:

   ```
   mkdir /mnt/rhel-dvd && mount /dev/cdrom /mnt/rhel-dvd
   ```

2. Create **rhel-dvd.repo** file in `/etc/yum.repos.d` directory (this file is required to contain paths to update packages).
3. Open **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
```

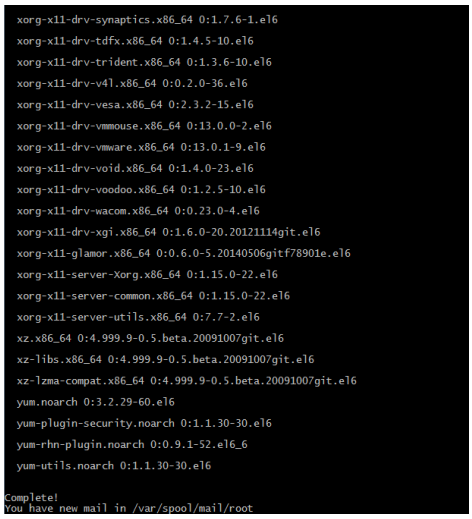
4. Save changed **rhel-dvd.repo** file.
5. Clean up packages manager cash:

   `yum clean all`

> **Warning!**
>
> Before updating from TM 5.1 to version 5.4 it is required to delete `iwtm-tmcap`:
>
> `rpm -e --nodeps iwtm-tmcap`
>
> Otherwise the `tmcap.ko` cernel's module can be deleted, which results in the need of reinstalling the new `iwtm-tmcap`.
>
> This step can be skipped updating DB Server.

6. Run packages update process:

   `yum update`



7. Check whether configuration files of new version with conf.epmnew extention are available in `/opt/iw/tm5/etc/` catalogue.
   - In case there are mentioned files in the directory, align them with the old configuration files.

3.2. Updating DB scheme

1. Connect to BD under scheme owner user:

   `su - oracle`

   `sqlplus`

> **Примечание:**
>
> Scheme owner user is `iwtm` by default.

2. Get list of scheduled jobs:

   `select JOB_NAME, STATE from user_scheduler_jobs u where u.enabled = 'TRUE';`

3. Disable jobs:

```
BEGIN
dbms_scheduler.disable('JOB_1',true);
dbms_scheduler.disable('JOB_N',true);
COMMIT;
END;
/
```

where `JOB_1... JOB_N` – names of active jobs.

4. Make sure, there are no jobs running at the moment:

```
SELECT job_name FROM user_scheduler_running_jobs ;
```

   - In case a job is running, stop it:

```
BEGIN
dbms_scheduler.stop_job('JOB_NAME');
COMMIT;
END;
/
```

     where `JOB_NAME` – name of a job.

5. Disconnect users from DB.
6. Stop services, which could have access to DB:

```
service iwtm stop
service php-fpm stop
service nagios stop
```

> **Note:**
>
> In case there is Crawler subsystem installed in the System, it is required to stop processes of the mentioned subsystem (on Crawler Server).

7. Make sure, that database.conf has been updated correctly and has current scheme version mentioned:

```
less /opt/iw/tm5/database/database/database.conf
```

8. Go to /`opt/iw/tm5/database/database/` directory:

```
cd /opt/iw/tm5/database/database/
```

9. Run DB update using script:

```
./update.sh
```

10. Start the services:
11. `service iwtm start`
12. `service php-fpm start`
13. `service nagios start`

> **Note:**
>
> In case there is Crawler subsystem installed in the System, it is required to start processes of the mentioned subsystem (on Crawler Server).

14. Start the stopped jobs:

```
BEGIN
dbms_scheduler.enable('JOB_1');
dbms_scheduler.enable('JOB_N');
COMMIT;
END;
/
```

where JOB_1... JOB_N – names of the stopped jobs.

CHAPTER 4. UNINSTALLING THE SYSTEM

In this chapter:

- *Database Schema (i. 4.1 on page 56).*
- *Remote Database Management Module (i. 4.2 on page 57).*
- IW ICAP Module (i. 4.3 on page 57).
- *Traffic Monitor Server (i. 4.4 on page 57).*
- *Sniffer (i. 4.5 on page 58).*
- *Crawler (i. 4.6 on page 58).*
- *Web-console (i. 4.7 on page 58).*

4.1. Database Schema

> **Warning!**
>
> Do not uninstall the database schema from which daily tablespaces were detached for archival purposes. Otherwise you will not be able to recover data from these tablespaces.

1. Verification of Oracle DBMS server

Make sure that:

- Version of database schema installed matches version of software package used for its removal.
- The Oracle DBMS server is running;
- Login and password for account with SYSDBA permissions (`sysdba` and `sysdba_password` setting values) are correctly specified in `database.conf` file.

2. Stopping Traffic Monitor

Before uninstalling you need to:

- Stop all Traffic Monitor Server processes:

  ```
  service iwtm stop
  ```

- Close all Management Console instances;
- Stop WEB-service:

  ```
  service php-fpm stop
  ```

- Stop all connections to deleted database schema from other programs.

3. Launch of schema deletion

Go to /`opt/iw/tm5/database/database`/ directory.

Run the script:

```
./uninstall.sh
```

4.2. Remote Database Management Module

To uninstall the remote database management module:

1. On the computers where client and server parts of module are installed, run the following command:

   ```
   rpm -e iwtm-qmover
   ```

   If configuration file (`qmover.conf`) was changed during operations, it will be saved to the computer as `qmover.conf.rpmsave` after uninstalling the module.

2. On the client side (the interceptor of objects), from cron, delete all settings which change the bandwidth of the data transmission channel. For more information see «*InfoWatch Traffic Monitor. Administration guide*»).

4.3. IW ICAP Module

If interception of HTTP requests over the ICAP protocol is no longer required you may disable IW_ICAP module.

To disable the IW_ICAP module:

1. Stop Traffic Monitor server processes:

   ```
   service iwtm stop
   ```

Disable autorun of `iw_icap` process (for more information on enabling and disabling processes autorun see «*InfoWatch Traffic Monitor. Administration guide*»).

2. Start Traffic Monitor server processes:

   ```
   service iwtm start
   ```

3. Check the status of Traffic Monitor processes:

   ```
   service iwtm status
   ```

Restore the original proxy settings

If required, you can delete the rpm package of `iwtm-icap`.

To delete the rpm package of the IW ICAP module:

run the command:

```
rpm -e iwtm-icap
```

If configuration file (`qmover.conf`) was changed during operations, it will be saved to the computer as `qmover.conf.rpmsave` after uninstalling the module.

4.4. Traffic Monitor Server

Before uninstalling server part of Traffic Monitor you must uninstall:

- Remote database management module (i. 4.2 on page 57 - both client and server part of the module) – if Traffic Monitor server was used to load objects to remote database..
- IW ICAP module (i. 4.3 on page 57) – if HTTP traffic was intercepted through integration with ICAP server.
- InfoWatch DeviceLock Adapter module – if it was installed as part of Traffic Monitor package to receive objects from DeviceLock. See recommendations for uninstalling in *"InfoWatch DeviceLock Adapter. Installation and Configuration Guide".*

To uninstall Traffic Monitor server:

1. Run the following command:

   ```
   rpm -e `rpm -qa | grep iwtm`
   ```

2. Reconfigure traffic interception components configured on Traffic Monitor.

The traffic interception schema in InfoWatch Traffic Monitor	Required steps after InfoWatch Traffic Monitor is uninstalled
Intercepting a Copy of SMTP Traffic (Using a Mail Relay Server)	Make sure that the parameters of Postfix are restored to its initial state
SMTP traffic is intercepted and filtered by the System (integration with Postfix)	Make sure that the parameters of Postfix are restored to its initial state. Configure SMTP emails to be delivered by the corporate mail server and bypass InfoWatch Traffic Monitor.

After uninstalling, these elements remain on the computer:

- Modified configuration files.
- `The .rpmsave` suffix is added to modified files (for example, `detector.conf.rpmsave`). The unchanged files will be deleted.
- Object queue.
- Classification.
- The license file.
- Account of the user who own InfoWatch Traffic Monitor and the group which this user belongs to.

If the integration with Postfix was performed then the rollback to initial settings is performed while uninstallation.

4.5. Sniffer

If the Sniffer and other Traffic Monitor Server components are installed on the same computer, Sniffer will be uninstalled together with Traffic Monitor (see i. Traffic Monitor Server on page 57). A special uninstallation procedure is not required in this case.

To uninstall Sniffer installed separately from other Traffic Monitor components:

run the command:

```
rpm –e iwtm-sniffer
```

4.6. Crawler

Crawler subsystem (**Server** as well as **Scanner**) can be deleted by standard Windows means: **Start -> Control Panel -> Programs and components**, command **Delete**.

4.7. Web-console

As management with the help of the web console is being performed via web-browser, no additional steps to uninstall web-console are required.

4.8. InfoWatch Lync Adapter

Deletion of InfoWatch Transfer Service 1.0 and IW OCS Filter 2.0 is being performed by standard Windows means using Control Panel.

Appendix 1. USER NAME AND PASSWORD RECOMMENDATION

Rules for logins

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

Rules 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 «_».

  It should start with a letter only.
- The password is case-sensitive.

Recommendations for strong passwords

- Recommended password length is 10-30 characters.
- The password must contain both 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

Do not start user names or passwords with these combinations: SYS_ and ORA_.

Do not use 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

Appendix 2. THIRD-PARTY LICENSES

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 contains 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 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

GLOSSARY

Active Directory

LDAP-compatible implementation of Microsoft smart directory service for Windows operating systems

Administrator

Pre-installed role and Management Console account that has privileges for managing other accounts and their rights. Also - system user performing installation, configuration and supporting operation of System. See also: Security Officer

Authorization engine

Transfer method and contents of user data that is passed by HTTP client to proxy

BCC

Blind Carbon Copy. Technique that enables sending a copy of message to another recipient (in addition to main recipient) without any indications to it in original message.

Cluster

Group of PCs sharing the same set of installed components which is arranged and used as a common resource. See also: Component

Component

System software unit that may be installed independently from other System parts

Copy mode

Transport Mode attribute value. In this mode only the copy of traffic is passed through the System, not the real traffic, therefore, the feature to block traffic with System tools is unavailable. See also: Transport Mode, Interception Mode

Crawler

Traffic Monitor Subsystem which allows files scanning for violations of corporate security policies inside the corporate network. Therefore InfoWatch Crawler allows to monitor file resources for detecting and preventing unauthorized usage of confidential data.

Daily tablespace

One of tablespace types in InfoWatch Traffic Monitor database. Used to store data intercepted within 24 hours (intercepted objects, analysis & object processing results). Daily tablespaces are being created every day in such a way that the database always has a tablespace for the next two days.

Data Interception

Retrieval, parsing, classification and conversion of data (or copies of data) into context. Interception is performed for data passed via SMTP, HTTP, ICQ/OSCAR, IXP protocols. See also: Data Transfer Channel, Interceptor

Data Transfer Channel

Environment containing technical facilities for data transfer, software tools and data transfer protocols. Traffic Monitor supports intercepting data in the following data transfer channels: email (SMTP), web (HTTP), instant messengers (ICQ), shadow copies of files and workstations connection/disconnection events, print jobs.

DB

Database.

DBMS

Database management system

Device Monitor

Traffic interception module. Software designed for managing user access to peripherals and monitoring operations that involve copying files to removable storage media and sending them to printer. Allows to proceed a copy of HTTPS, MAPI and FTP traffic and copy of messages from Skype, Yahoo, GTalk and Mail.Ru Agent messengers.

DeviceLock

Software complex developed by ZAO “Smart Line Ink” that controls user access to peripherals and local PC ports

DeviceLock Adapter

Traffic interception module. Interceptor that passes shadow copies (created by DeviceLock system (Smart Line Ink)) of files transferred to external data carriers and sent to printer, to the Traffic Monitor. See also: Device Monitor, Shadow copy, Interceptor, DeviceLock

ICAP

Internet Content Adaptation Protocol – protocol enabling control of inbound/outbound HTTP-traffic. Enables modifying HTTP requests contents (only outbound traffic within InfoWatch Traffic Monitor). See also: ICAP Client, ICAP Server

ICAP Client

Component installed on proxy supporting ICAP features. Passes HTTP request or response, encapsulated in ICAP-message, to ICAP server. Receives ICAP server response (skip/block HTTP-request). See also: ICAP

ICAP Server

Server component receiving HTTP requests encapsulated in ICAP message. Retrieves HTTP requests from ICAP message and pre-processes them. Passes response with processing results to ICAP client. See also: ICAP

InfoWatch Traffic Monitor

InfoWatch Traffic Monitor (IW TM) software complex. Designed for control of various informational data transfer channels (SMTP, HTTP, ICQ. In Traffic Monitor Enterprise – also data copied to removable data carriers and sent to printer). See also: Traffic Monitor Enterprise, Traffic Monitor Standard

Integration with Postfix

Configuring Postfix mail server usage as a relay server in the schema of intercepting SMTP-traffic copy. See also: Postfix

Interception mode

Method of processing traffic by Traffic Monitor: processing real traffic or traffic copy. In the first case Traffic Monitor receives real traffic, and intercepted objects are only sent for further processing after they are processed and decision is made. In the second scenario Traffic Monitor received copy of traffic, and Traffic Monitor has no impact on sending intercepted objects. See also: Data Transfer Channel, Interceptor, Object

Interceptor

Software retrieving data from external clients, provisioning the data for further analysis and passing them to Processing subsystem. See also: Data Transfer Channel

LDAP

Lightweight Directory Access Protocol – network protocol for access to X.500 directory service using TCP/IP

Mail agent

Aka MTA (Mail Transfer Agent) Message forwarding agent, mail server – software that transfers mails between computers.

Management Web-Console

Graphic user web-interface. Designed for managing InfoWatch Traffic Monitor (administrating the System, configuring settings, analyzing objects, etc.).

Normal transport mode

Transport Mode attribute value. In this mode real traffic is passed through the System, and the feature to block objects banned by the System is available. See also: Transport Mode, Interception Mode

Object

Data retrieved by the System from intercepted traffic (SMTP message, HTTP-requests, ICQ messages) or from external systems (shadow copies of files and print jobs) and converted by Processing subsystem into a internal view.

OCR

Optical Character Recognition is the process of conversion of images containing typewritten or printed text into machine-encoded text that can be used in text editor. Provides the analyzing of extracted text data.

OSCAR

Open though not free network protocol that enables instant & offline messaging. It is used by ICQ and AIM instant messengers.

Postfix

Mail agent (MTA) that you can integrate to intercept and deliver SMTP traffic within the System. See also: Mail Agent

Print jobs

Information on sending data for printing together with printed document

Processing Objects

Intercepted object parsing procedure that converts the object into context and assigns some attributes to it.

Proxy

Service for transferring data between client computers and network servers. Used by the System during interception of HTTP traffic.

Relay server

Broadcasting server. System may retrieve SMTP-traffic from a mail relay-server

Security Officer

Preset role and management console account that has all the privileges. See also: Administrator

Shadow copy

A copy of the file which is created on a removable storage media. The copy is created only if the file is successfully saved to the removable storage device.

Sniffer

Network traffic analyzer. Interceptor, InfoWatch Traffic Monitor component, retrieving data (SMTP, HTTP, ICQ traffic) of traffic copy, passing through SPAN-port of the switch and transferring them to Processing subsystem. See also: Data Transfer Channel, Interceptor

SPAN

Switched Port Analyzer – technique that enables mirroring traffic from one port to another

SPAN copy

Implementing interception mode for CISCO switch traffic copy. Enables operation of “Copy” transport mode. See also: Interception Mode, SPAN, Copy Mode,

System

See: InfoWatch Traffic Monitor

Traffic

Information flow within communication system. Within InfoWatch Traffic Monitor only outbound traffic is screened, that is passed via SMTP, HTTP and ICQ protocols.

Traffic Monitor Enterprise

InfoWatch Traffic Monitor edition that provides the full System functionality.

Traffic Monitor Server

Computer or aggregation of computers where InfoWatch Traffic Monitor components are located, except management console and database. See also: Management Console

Traffic Monitor Standard

InfoWatch Traffic Monitor edition that provides the limited System functionality. Specifically it enables interception of data in copy mode only; doesn’t support detecting text objects and digital prints or working with responsibility zones. See also: Copy Mode, Responsibility Zone

Transparent transport mode

Transport Mode attribute value. In this mode real traffic is passed through the System, but the feature to block objects banned by the System is unavailable. See also: Transport Mode, Interception Mode

Transport Mode

Object attribute specified in a script. It should consider implemented interception mode; determines the way of further delivery for the object. See also: Interception Mode, Copy Mode, Normal Transport Mode, Transparent Transport Mode