

INFOWATCH

# InfoWatch Traffic Monitor

## Administration Guide

© AO “InfoWatch”

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

http://www.infowatch.com

23.12.2016

TABLE OF CONTENTS


1 Traffic Monitor Overview 7

1.1 InfoWatch Traffic Monitor Features 8
1.1.1 In Stream/At The Gateway Traffic Interception 8
1.1.2 Revision of Files from the Corporate Network 21
1.1.3 Processing Traffic, received from Third-party Systems 21

1.2 InfoWatch Traffic Monitor Components 21

1.3 Licensing 23

2 Configuring System After Installation 26

2.1 Configuring Time Synchronization 27

2.2 Configuring Sphinx in case of distributed installation 27

2.3 General settings 28
2.3.1 Configuring Server to work with SPAN, or Port Mirroring Technology 28
2.3.2 Intercepting traffic, transmitted via ICAP protocol 33
2.3.3 Configuring Inline Mode for Several Interceptors 42

2.4 Configuring traffic interception 43
2.4.1 Configuring SMTP Traffic Interception 44
2.4.2 Configuring POP3 Traffic Interception 55
2.4.3 Configuring HTTP Traffic Interception 55
2.4.4 Configuring HTTPS Traffic Interception 56
2.4.5 Configuring SMTP Traffic Interception 57
2.4.6 Configuring NRPC Traffic Interception 57
2.4.7 Receiving Objects Intercepted by InfoWatch Device Monitor 58
2.4.8 Revision of Files from the Corporate Network 58
2.4.9 Configuring IMAP4 Traffic Interception 58

2.5 Process autorun 59
2.5.1 Check of process autostart 59
2.5.2 Enabling and disabling autorun processes 61

2.6 Configuring OCR extractors 62

2.7 Configuring Email Notifications for Users and Employees 63

2.8 Limiting the number of events that can be found 64

2.9 Configuring InfoWatch Device Monitor Server 64
2.9.1 <applicationSettings> Section 65
2.9.2 <system.diagnostics> Section 70

2.9.3 Deleting Temporary Device Monitor Files 72

3 Working in Web-Console 73

3.1 Logging on and off the Web-Console Interface 73

3.2 Managing LDAP Catalogues Integration 74
3.2.1 Creating connection to server 75
3.2.2 Editing connection to server 76
3.2.3 Deleting connection to server 76
3.2.4 Running Synchronization with Server Manually 76

3.3 Managing System Users and their Roles 77
3.3.1 Users 77
3.3.2 Roles 81
3.3.3 Visibility Scopes 84

3.4 Managing Licenses 87
3.4.1 Checking License Validity 88
3.4.2 Installing a License 88
3.4.3 Deleting License 89
3.4.4 Requesting a License 89

3.5 Healthcheck 89
3.5.1 Configuring notifications 91

3.6 Managing Services 91
3.6.1 Running service 91
3.6.2 Stopping service 92
3.6.3 Restarting service 92
3.6.4 Saving service logs 92

3.7 Collecting the Diagnostic Data 93
3.7.1 Collecting the diagnostic Data in normal Mode 94
3.7.2 Collecting the diagnostic Data in extended Mode 94

3.8 User Actions Audit 94
3.8.1 Audit Events 95
3.8.2 Filtering by User 96
3.8.3 Filtering by Action 96
3.8.4 Filtering by Object 97
3.8.5 Filtering by Date 97

3.9 Integrity monitoring 97
3.9.1 Manual integrity monitoring 97
3.9.2 Automatic integrity monitoring 98
3.9.3 Accepting result as standard 98

3.10 Plugins 98
3.10.1 Adding plugin 100
3.10.2 Deleting plugin 100
3.10.3 Working with tokens 101

4 Configuring Crawler Interceptor 102

4.1 Configuring Network Access 103

4.2 Crawler Configuration Files 105
4.2.1 Configuration File of Crawler Server 105
4.2.2 Configuration File of Crawler Scanner 107
4.2.3 Выключение шифрования трафика между компонентами 108

4.3 Crawler Log Files 108

4.4 Automatic deletion of Crawler events 109

5 Monitoring 109

5.1 Monitoring Subsystem for Distributed Architecture 110
5.1.1 Configuring Connection to Device Monitor 110
5.1.2 Configuring Indicators Manually 111
5.1.3 Configuring Addresses of Time Synchronization Server for Monitoring Subsystem 111
5.1.4 Configuring Threshold Value for Load Indicator 112
5.1.5 Configuring Notifications 112

6 Administrating Database 114

6.1 Oracle 114
6.1.1 Routine Database Maintenance 115
6.1.2 Tablespaces in InfoWatch Traffic Monitor database 116
6.1.3 Managing Daily Tablespaces 117
6.1.4 Database Backup 125

6.2 Postgre SQL 131
6.2.1 Tablespaces in InfoWatch Traffic Monitor database 132
6.2.2 Managing Daily Tablespaces 132
6.2.3 Database Backup 140

7 Administrating the Server End of InfoWatch Traffic Monitor 143

7.1 Traffic Monitor Server Processes 144
7.1.1 List of Traffic Monitor Server End Processes 144

7.1.2 Using Traffic Monitor Server End Processes 147

**7.2 Setting Traffic Monitor Server End Configuration Files 149**
7.2.1 Common Configurable Settings of Configuration Files 149
7.2.2 Specific Configurable Settings of Configuration Files 151

**7.3 Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file) 169**

**7.4 Configuring Settings of Enclosures Archives Processing 170**
7.4.1 The extractors.conf Configuration File 170
7.4.2 The extractors.xml Configuration File 171

**7.5 Archiving a Mail Queue Directory 173**

**7.6 Logging System work 173**

**7.7 File queues 174**

**7.8 Recovering the System after Failures 176**

**7.9 Managing morphology languages 177**
7.9.1 Adding new morphology language 178
7.9.2 Updating installed morphology language 178
7.9.3 Deleting morphology language 179

**7.10 Configuring serman.conf when changing DB Server Address 179**

**7.11 Configuring Forwarding Data to SIEM 180**
7.11.1 Configuring SIEM side 180
7.11.2 Configuring TM side 190
7.11.3 Type of logs, transmitted to SIEM 193

**7.12 Deleting temporary files 194**

## 8 Appendix A. User Name and Password recommendations 194

## 9 Appendix B. Monitoring indicators 197

### Introduction

This guide provides information on InfoWatch Traffic Monitor administration: configuration of the system after installation, disaster recovery, routine maintenance.

### Who Should Read this Guide

The guide is intended for InfoWatch Traffic Monitor Server administrators, which are familiar with the basics of Microsoft Windows and Linux and have the skills of Oracle and Postgre SQL DBMS administration.

### 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.

### 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), 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.

# Traffic Monitor Overview

In this chapter:

- InfoWatch Traffic Monitor Features;
- InfoWatch Traffic Monitor Components;
- Licensing.

## 1.1 InfoWatch Traffic Monitor Features

InfoWatch Traffic Monitor enables controlling data traffic in corporate networks in order to detect and prevent unauthorized use of confidential data.

- Interception of traffic transferred in stream/at the gateway via SMTP, POP3, HTTP, HTTPS, OSCAR (ICQ), NRPC (IBM Notes);
- Analysis of Skype traffic (text and audio), file shadow copies and print tasks, FTP traffic, Jabber (XMPP protocol), Mail.Ru Agent (MPP protocol) messengers control;
- Revision of files within a corporate network;
- Processing traffic, received from third-party systems;
- Analysis of the intercepted traffic content to detect corporate policy and security violations;
- Filtering intercepted traffic by means of allowing or prohibiting deliverance of particular data.

### 1.1.1 In Stream/At The Gateway Traffic Interception

The chapter contains information about traffic types and their interception schemes:

- SMTP Traffic Interception Scheme;
- POP3 Traffic Interception Scheme;
- HTTP Traffic Interception Scheme;
- HTTPS Traffic Interception Scheme;
- ICQ Traffic Interception Scheme;
- NRPC Traffic Interception Scheme;
- IMAP4 Traffic Interception Scheme;
- Other interception channels.

#### SMTP Traffic Interception Scheme

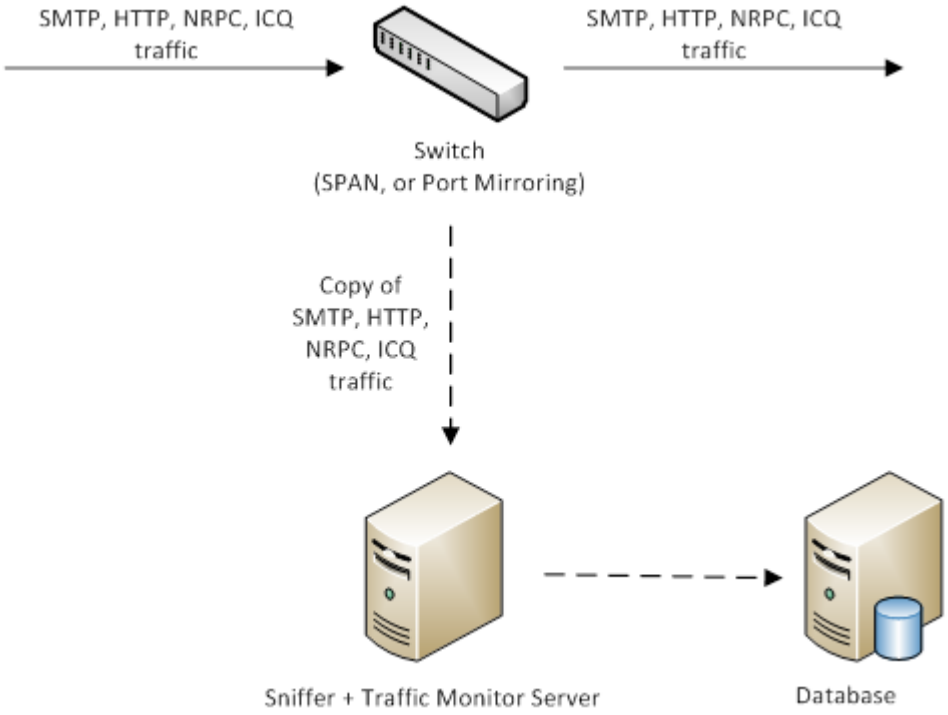
**Method 1:**

Traffic is being intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

Big number of managed network switches will allow duplicating traffic from one, several ports or VLAN on an individual port.

In this case customized switch port is being attached to Traffic Monitor Server network interface. Server interface is being switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror internal switch port or internal proxy-server interface.




For more information on functionality *see* "SPAN, or Port Mirroring"

**Advantages:**

- This method allows to analyze traffic safely even in the isolated network segment. System can never influence analyzed traffic, regardless of Server state.
- SMTP traffic of external servers is being analyzed as well (for example, Mail.ru traffic, given that SMTP protocol is being used)

**Shortcomings:**

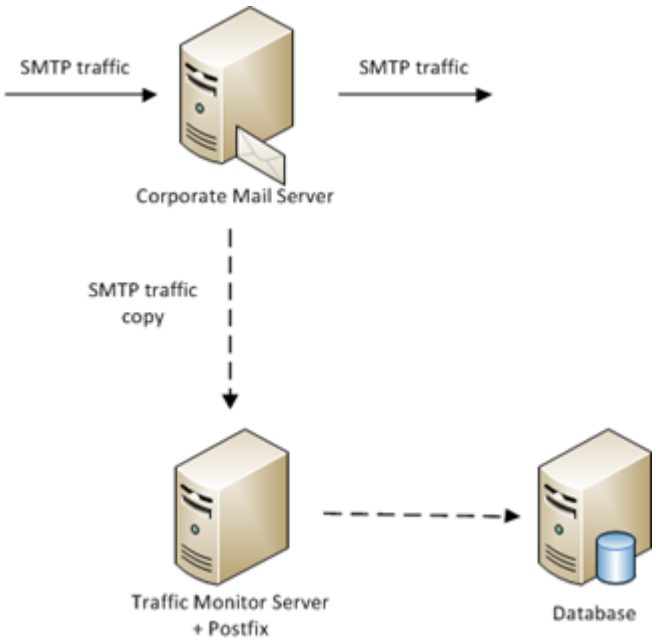
Under heavy load of switch, packages can be partially lost, especially, when the traffic is being mirrored from two ports to one, therefore we need:

- switch with corresponding functionality;
- additional network adapter on monitoring server.

Among shortcomings, internal communications are not being controlled.

**Method 2:**

On a corporate mail server it is necessary to setup a rule, sending shadow copy (BCC) for each sent message. Copy should be sent to mail address with mail domain, which has the same IP-address as Traffic Monitor Server. Most mail servers have such functionality.




For more information on functionality see *"Recieving Copies from Mail Server"*

**Advantages:**

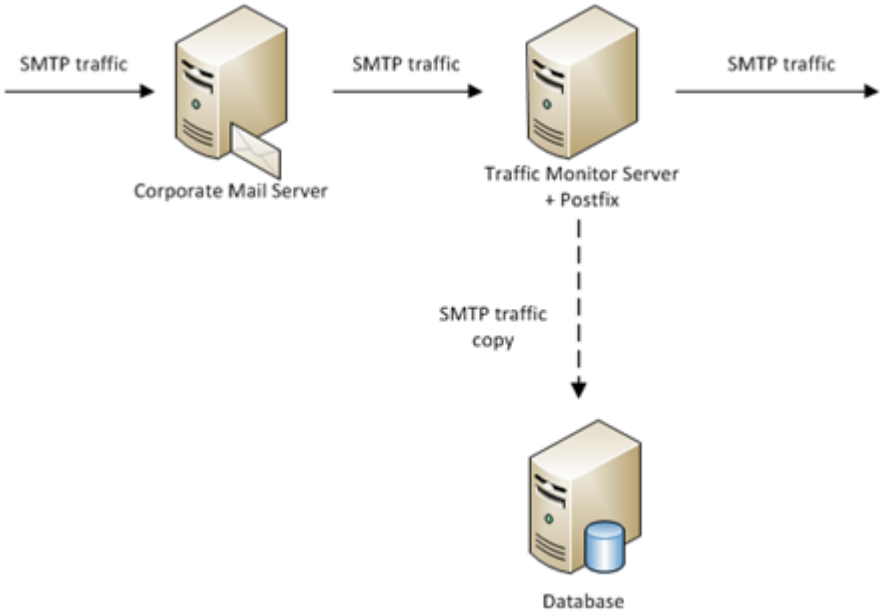
- Apart from external, allows to analyze company internal communications;
- When MS Exchange 2007 or newer is used there is functionality to analyze communications of a certain user group;
- Guarantees entire mail analysis.

**Shortcomings:**

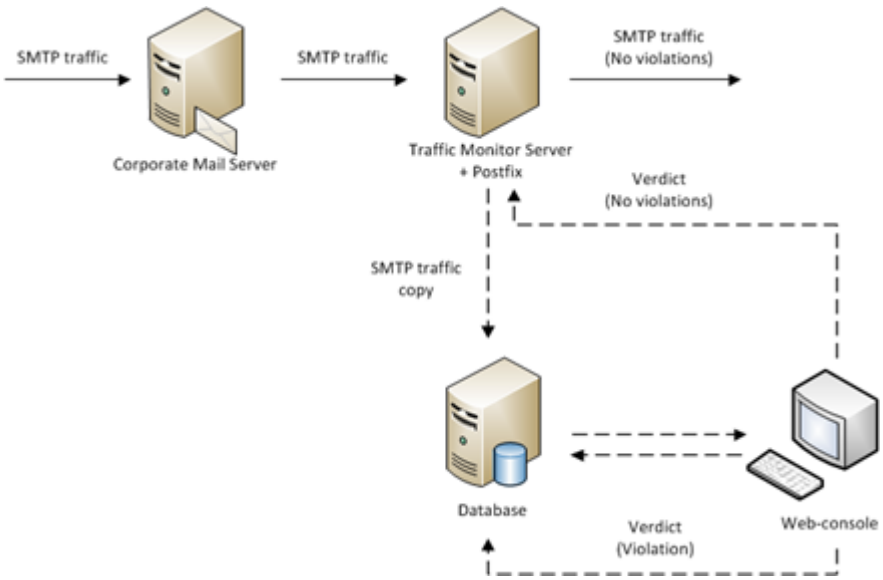
- Requires settings of a corporate mail server to be changed;
- External mail servers (in case allowed) is not being controlled;
- Upon Traffic Monitor Server inaccessibility, users will receive mail about shadow copy delivery error;
- Additional mail server load.

**Method 3:**

Monitoring server is being used as an intermediate mail server. Monitoring server includes Postfix mail server.




Copy




Block

For more information on functionality see *"Inline Mode"*.

**Advantages:**

Allows enabling mail traffic block functionality.

**Shortcomings:**

- Requires settings of a corporate mail server to be changed;
- External mail servers (in case allowed) is not being controlled;

Upon monitoring server inaccessibility, users cannot send mail, in case server reservation has not been provided (for example, through MX-records).

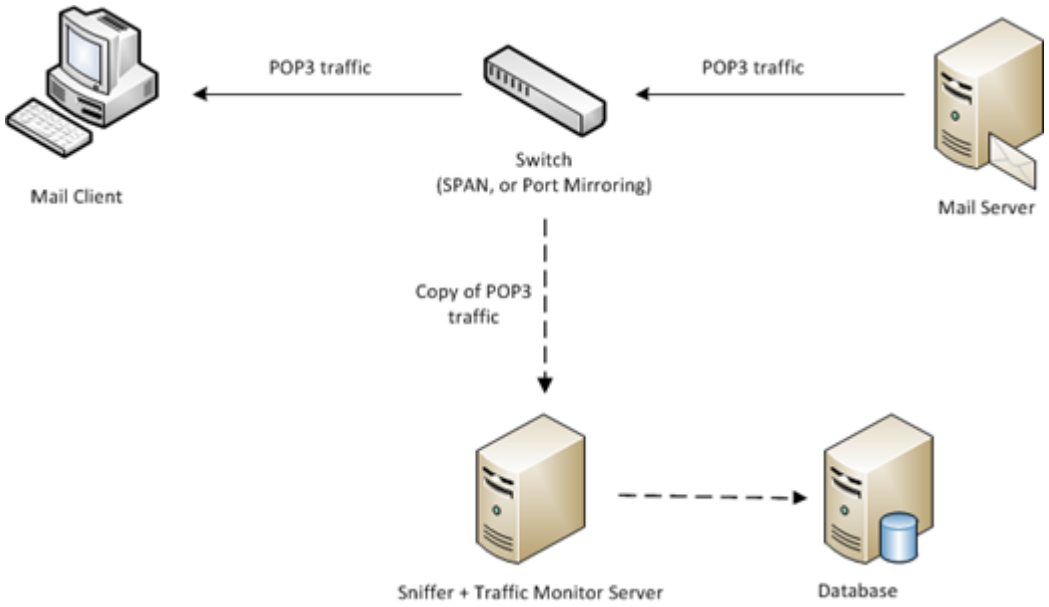
## POP3 Traffic Interception Scheme

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror the internal switch port or internal proxy-server interface.




For more information on functionality see "Configuring POP3 Traffic Interception".

## HTTP Traffic Interception Scheme

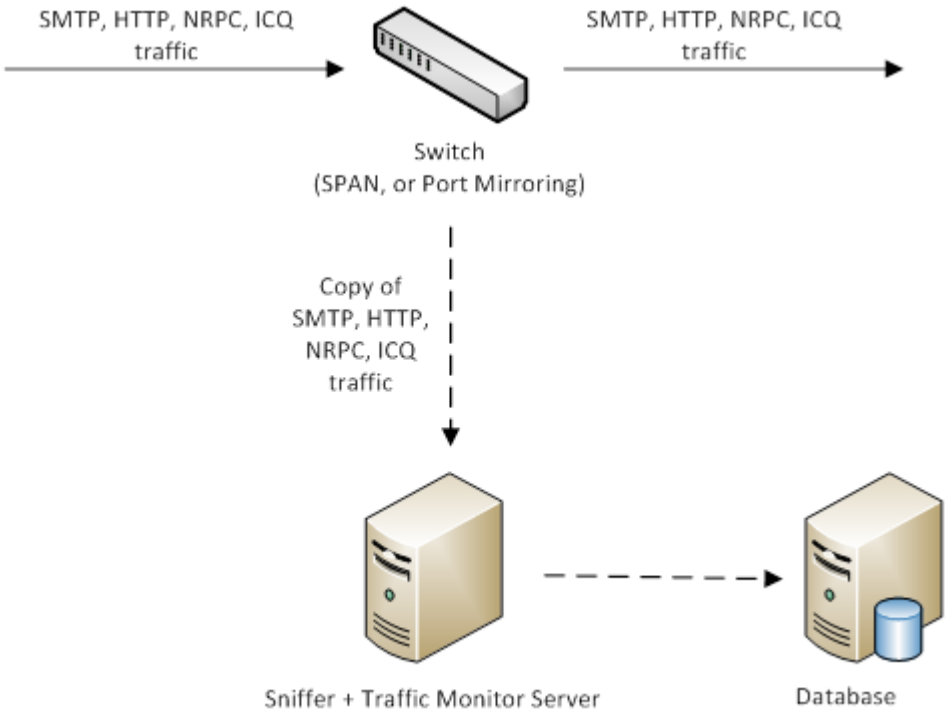
**Method 1:**

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror the internal switch port or internal proxy-server interface.




For more information on functionality see *"SPAN, or Port Mirroring"*.

**Advantages:**

- This method allows to analyze traffic safely even in the isolated network segment. System can never influence analyzed traffic, regardless of Server state.

**Shortcomings:**

- Under heavy load on the switch, some packages can be lost, especially, when the traffic is mirrored from two ports to a single port. To prevent the loss of packages, you should use:

- a switch with corresponding functionality;

- an additional network adapter on the monitoring server.

**Special case 1:**

In case monitoring server is located in virtual environment, in addition to switch port setup, to monitor traffic an individual virtual switch is being created with promiscuous mode enabled. Switch should be connected to an individual physical interface. This method allows you to analyze the traffic of virtual machines running through a virtual switch.

This method works on VMware ESXi servers. On Hyper-V this functionality is implemented with limitations starting with version 2012 Hyper-V.

**Special case 2:**

Instead of managed switch, HUB can be used. This variant's disadvantage is HUB device's is low transmission capacity, as well as inability to buy a device in connection to removal from production.

**Method 2:**

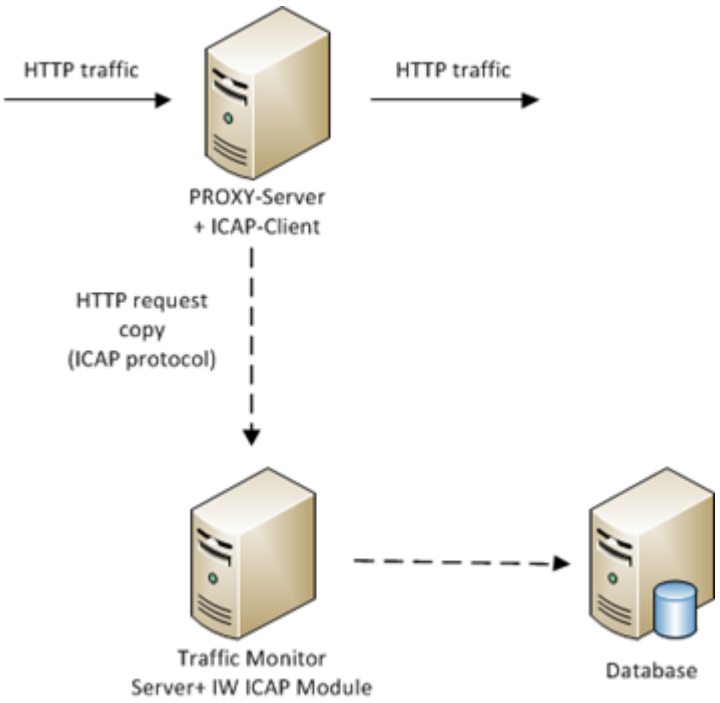
Traffic copy, which is transmitted via ICAP protocol, is intercepted from corporative proxy-server.

Traffic Monitor Server is positioned as an ICAP client. In case there is a proxy-server in company, which supports ICAP protocol, it is possible to use this functionality for analysis of HTTP traffic.

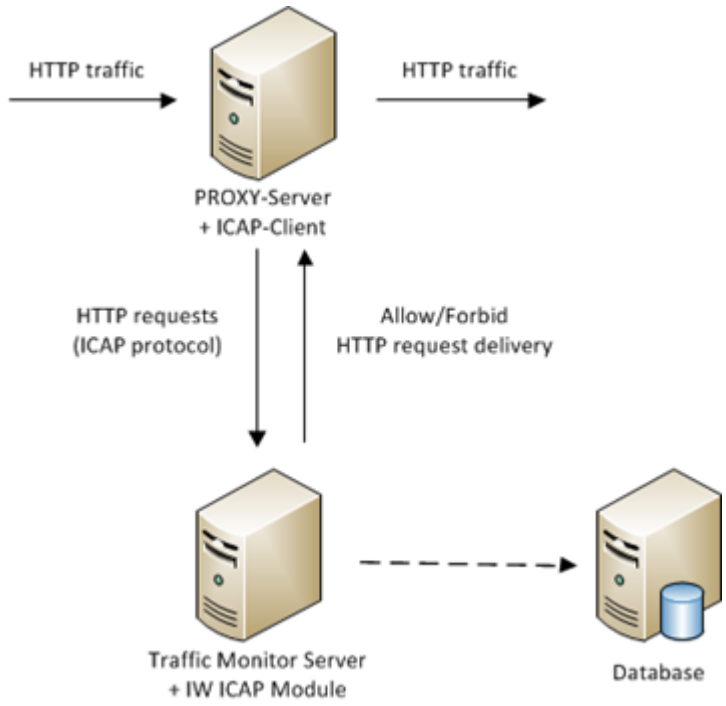
The following proxy-servers support this option:

- Cisco Ironport
- SQUID (given that the package has been compiled including ICAP support)
- Blue Coat SG
- MDaemon
- Zimbra ZCS
- Microsoft Forefront Threat Management Gateway 2010 SP2 (web-filter installation is required)

> **Note:**
>
> Working with other proxy-servers which maintain ICAP is possible, but requires preliminary compatibility test.




Copy




Block

For more information on functionality see "Inline Mode".

**Advantages:**

- Guarantees all packages delivery;
- Traffic Monitor Server can work in blocking mode («inline») with some proxy-servers.

**Shortcomings:**

- Proxy-server with corresponding functionality is required;
- Additional proxy-server load;
- Changing corporate proxy-server setup;
- Slight increase in the response time of Internet resources is possible.

## HTTPS Traffic Interception Scheme

> **Warning!**
>
> All methods of analyzing HTTPS traffic should be used with caution. The technology of analyzing HTTPS traffic is based on replacing a certificate of HTTPS session with a certificate issued by the proxy server (**man-in-the-middle attack**). On the user PC, the certificate must be considered a trusted one; otherwise, it will not be able to connect to an HTTPS resource. All HTTPS resources, which use personal certificates for identification (e. g., different client banks), must be excluded from interception.

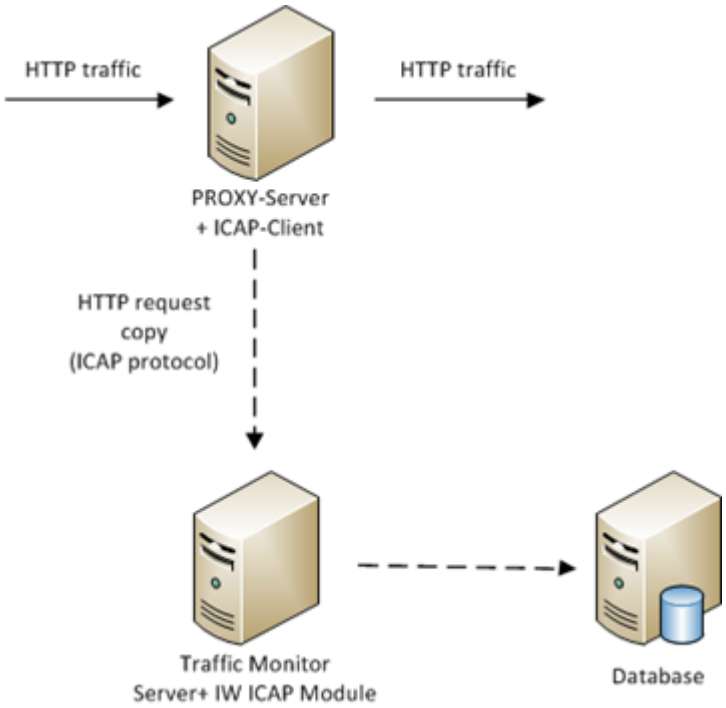
**Method 1:**

Corporate proxy-server carries out certificate replacement and HTTPS traffic parsing. After parsing HTTPS traffic, the proxy server sends traffic as HTTP to Traffic Monitor Server via ICAP protocol.

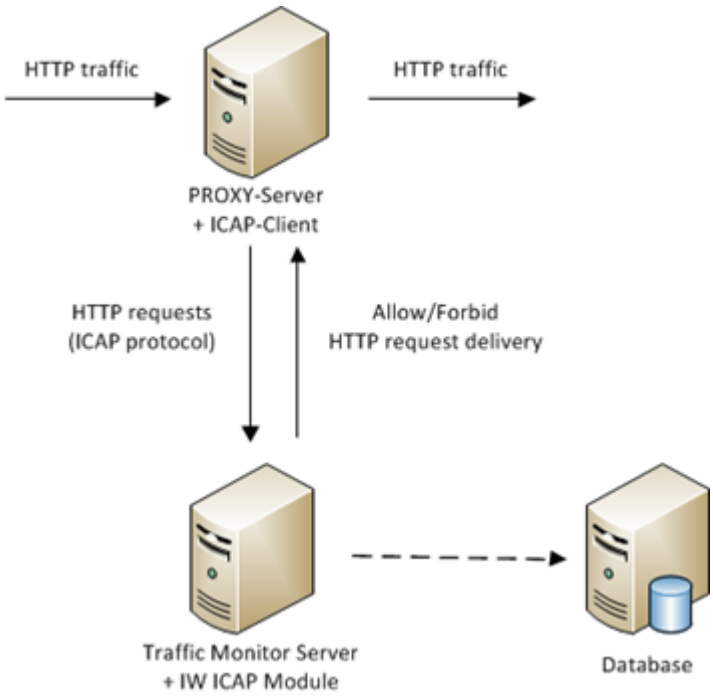
The following proxy servers support this option:

- Cisco Ironport
- SQUID (given that the package has been compiled including ICAP support)
- Blue Coat SG
- MDaemon
- Zimbra ZCS
- Microsoft Forefront Threat Management Gateway 2010 SP2 (web-filter installation required)

> **Note:**
>
> Working with other proxy servers, which maintain ICAP, is possible, but requires preliminary compatibility test.




Copy




Blocking

For more information on this functionality, see *"*Inline Mode*"*.

**Advantages:**

- Entire HTTPS traffic is analyzed.

**Shortcomings:**

- It is necessary to take into consideration needs of all proxy-server users;
- Additional load on a proxy server;
- Need to make some preparations which include creating exclusions list and certificate distribution.

**Special case:**

InfoWatch engineers can install a free SQUID proxy server on the Traffic Monitor Server.

**Advantages:**

- It is possible to analyze HTTPS.

**Shortcomings:**

- SQUID engineer is required to maintain the service.

**Method 2:**

HTTPS traffic analysis is performed by InfoWatch Device Monitor.

*For more information on this functionality see «InfoWatch Device Monitor. User guide».*

**Advantages:**

- An agent automatically puts its certificate to the trusted ones;
- Analysis of HTTPS traffic in company environment can be introduced gradually.

**Shortcomings:**

- Needs of a particular PC user should be taken into consideration.

## ICQ Traffic Interception Scheme

Intercepting the copy of ICQ traffic (OSCAR protocol) which passes through equipment with SPAN technology support. ICQ traffic interception is possible over HTTP.

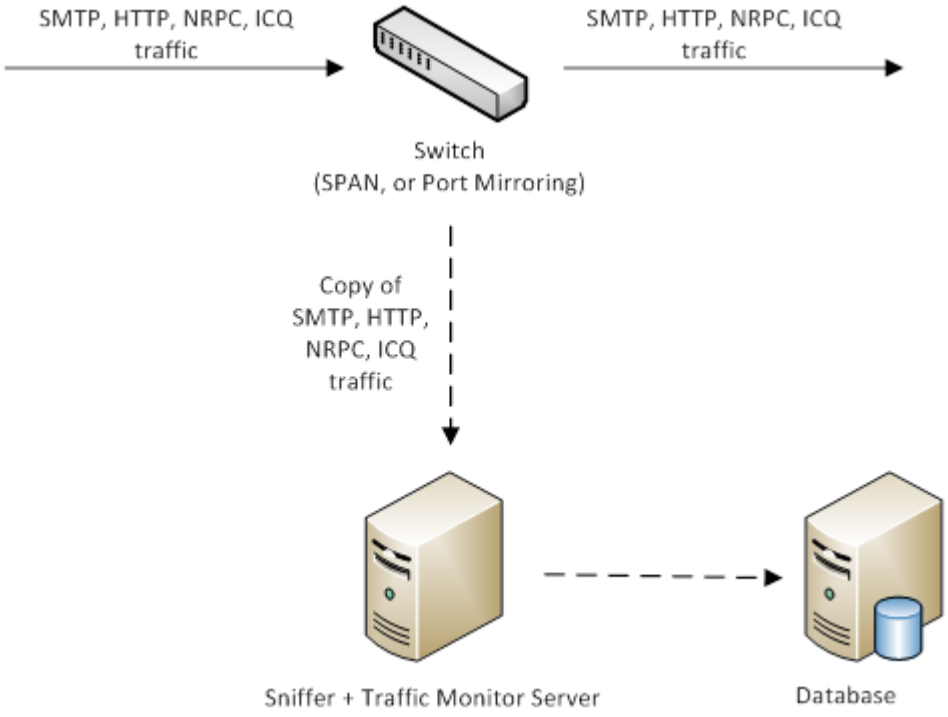
> **Warning!**
>
> Interception and analysis of encrypted ICQ traffic (including traffic transferred via SSL protocol) is not supported.

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror internal switch port or internal proxy-server interface.




For more information on functionality see "SPAN, or Port Mirroring".

**Advantages:**

Allows analyzing traffic safely even in an isolated network segment. System cannot influence the traffic being analyzed regardless of the Server state.

**Shortcomings:**

Under heavy load on the switch, some packages can be lost, especially, when the traffic is mirrored from two ports to a single port. To prevent the loss of packages, you should use:

- a switch with corresponding functionality;
- an additional network adapter on the monitoring server.

## NRPC Traffic Interception Scheme

NRPC traffic copy interception (used in IBM Notes System) which passes through equipment with SPAN technology support.

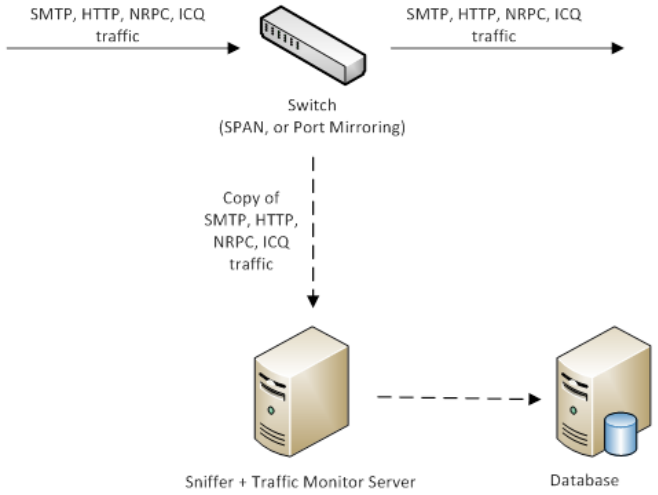
**Method 1:**

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror internal switch port or internal proxy-server interface.




For more information on functionality see "SPAN, or Port Mirroring"

**Advantages:**

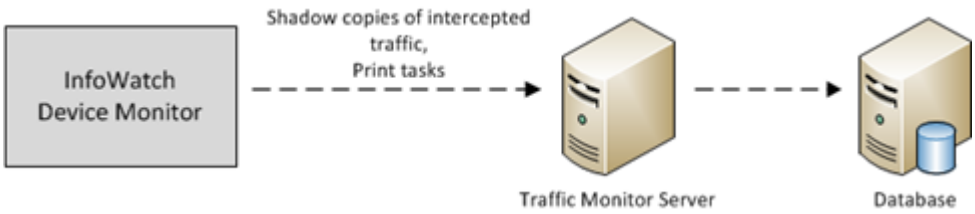
Allows analyzing traffic safely even in an isolated network segment. System cannot influence the traffic being analyzed regardless of the Server state.

**Shortcomings:**

Under heavy load on the switch, some packages can be lost, especially, when the traffic is mirrored from two ports to a single port. To prevent the loss of packages, you should use:

- a switch with corresponding functionality;
- an additional network adapter on the monitoring server.

## Other interception channels




On client OS Microsoft Windows XP SP3 and newer or mobile devices powered by Android and iOS one can install Device monitor Agents, which perform the following steps:

- realtime monitoring of managed computers (see article "Configuring Device Monitor Rule");
- monitoring computer print operations (see article "Configuring Print Monitor Rule");
- supervising Instant Messengers: Skype, WhatsApp, Jabber (XMPP protocol) and Mail.Ru Agent (MMP protocol) (see article "Configuring IM Client Monitor Rule");
- supervising SMS of mobile communication (see article "Configuring IM Client Monitor Rule");
- supervising traffic transferred by FTP and FTPS (see article "Configuring FTP Monitor Rule");
- supervising data transferred to external and external devices (see article "Configuring Network Monitor Rule");
- supervising photographs made by cameras of mobile devices (see article "Configuring Photo Monitor Rule");
- Microsoft RDP and Citrix ICA client control (see article "Configuring Device Monitor Rule");
- cloud storage control (see article "Configuring Cloud Storage Monitor Rule");
- screenshot control (see article "Configuring ScreenShot Control Monitor Rule");
- application control (see article "Configuring Application Monitor Rule").

All intercepted data can be transferred to Traffic Monitor for further analysis.

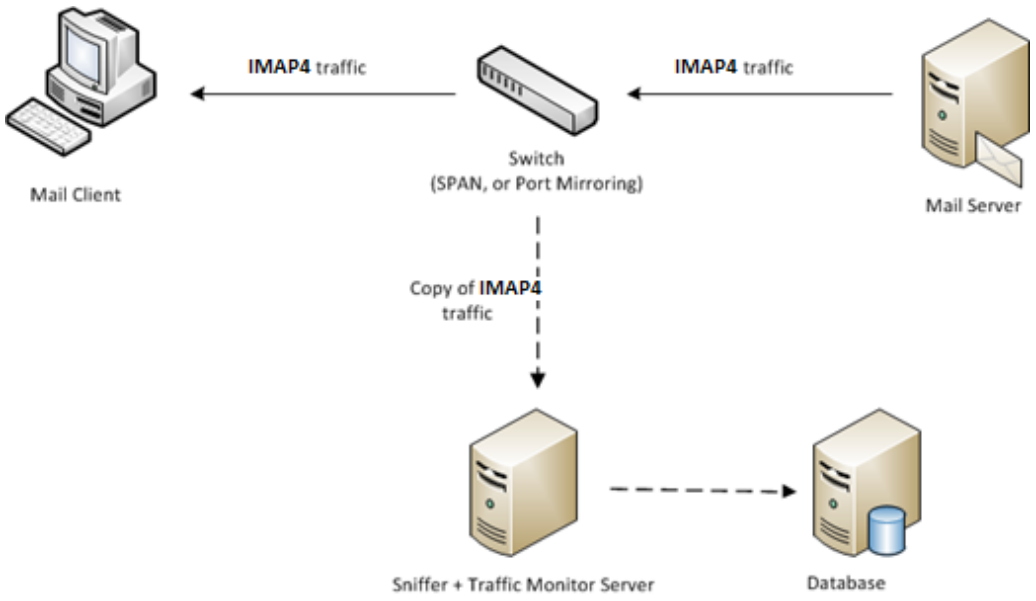
## IMAP4 Traffic Interception Scheme

Traffic is intercepted from a managed switch by using SPAN Port, or Port Mirroring technology.

A large number of managed network switches allow duplicating traffic from one or several ports or VLAN to a single port.

In this case customized switch port is connected to Traffic Monitor Server network interface. Server interface is switched to promiscuous mode, which allows accepting all incoming packages. This interface does not require an IP-address.

It is most effective to mirror the internal switch port or internal proxy-server interface.




For more information on functionality see *"SPAN, or Port Mirroring"*.

### 1.1.2 Revision of Files from the Corporate Network

File server and network resources content analysis is possible after installing special module on MS Windows Server.

For more information on functionality see "Configuring Crawler Interceptor".

### 1.1.3 Processing Traffic, received from Third-party Systems

Traffic Monitor supports number of adapters, which work under the scheme of data transfer from integrable systems and storing it in a database:

- **InfoWatch DeviceLock Adapter**. Find recommendations for installation and administration in document "InfoWatch DeviceLock Adapter. Installation and administration guide";
- **InfoWatch IRM Adapter**. Find recommendations for installation and administration in document "InfoWatch IRM Adapter. Installation and administration guide";
- **InfoWatch Lotus Domino Adapter**. Find recommendations for installation and administration in document "InfoWatch Lotus Domino Adapter. Installation and administration guide";
- **InfoWatch MS Lync Adapter**. Find recommendations for installation and administration in document "InfoWatch MS Lync Adapter. Installation and administration guide";
- **InfoWatch TMG Adapter**. Find recommendations for installation and administration in document "InfoWatch TMG Adapter. Installation and administration guide";
- **InfoWatch Device Control Adapter**. Find recommendations for installation and administration in document "InfoWatch Device Control Adapter. Installation and administration guide";
- **InfoWatch Cisco UCM Adapter**. Find recommendations for installation and administration in document "InfoWatch Cisco UCM Adapter. Installation and administration guide".

# 1.2 InfoWatch Traffic Monitor Components

| **InfoWatch Traffic Monitor component** | **Purpose** |
|---|---|
| Traffic Intercepting subsystem | Intercepts the traffic (objects or copies of objects) and transfers it for processing.<br>Consists of the following modules:<br>• Sniffer module;<br>• ICAP module;<br>• Device Monitor module; |
| Processing subsystem | Retrieving significant information and attachments from intercepted objects, determining attachment formats and transferring retrieved texts to Analysis subsystem.<br>**Note:** together with an object, its XML context is created: a text file which includes object contents and information about the object. |
| Analysis subsystem | Analysis of text data retrieved from intercepted objects (texts of e-mails, messages, queries as well as text, retrieved from attachments).<br>Consists of the following technologies:<br>• Categories and terms;<br>• Text objects;<br>• Sample documents;<br>• Blanks;<br>• Stamps;<br>• DB unloadings;<br>• Graphical objects. |
| Policies Application subsystem | Based on results of Analysis and Processing subsystems operations, the Policies Application subsystem is making a decision on violation or non-violation of informational security by intercepted object. It also associates object recipient or sender data with reference records on employees & workstations.<br>Consists of the following modules:<br>• Active Directory Integration module;<br>• Decision Making module. |
| Storage subsystem | Storage of intercepted objects data, analysis and policy application results, and the ability to view stored information using management console queries. It is a database.<br>Consists of the following modules:<br>• Remote Database Management module; |

| InfoWatch Traffic Monitor component | Purpose |
|---|---|
| | • Uploading Objects to Database module;<br>• System Settings Storage module;<br>• Objects Storage module.<br>**Note:** before saving the object to the database, it is converted from one internal format (XML) to another one (LIRO) |
| Monitoring subsystem | Feature of remote tracking performance indicators of servers where InfoWatch Traffic Monitor components and related services are installed. Performing general management operations.<br>The administration works with the subsystem via the web interface. |
| Audit subsystem | Ability to configure search filters (by person, action, object, dates), receive visual information about events and violations according to installed filters, as well as define storage period in the System. The administration works with the subsystem via the web interface. |
| Management Console subsystem | Provisioning graphic user interface used to administrate, configure and use Traffic Monitor.<br>Consists of the following modules:<br>• Monitoring module;<br>• Control module;<br>• Configuration module. |

# 1.3 Licensing

Trial license for interceptors is valid for 30 days since Traffic Monitor distribution compilation and allows usage by not more than 100 users. To proceed with System exploitation, install commercial license for interceptors, which are planned to be used.
To proceed with System exploitation after trial period, install commercial license for interceptors, which you plan to use. To do this, request commercial license key file (see "Requesting license").
Commercial license key is a LIC format file.
Installing and using license key one should consider the following:

- In case trial license period has expired, interceptors work will be stopped. Install commercial license or uninstall the System.
- In case it is required to change traffic transmission parameters according to new deployment scheme, change license key considering new interceptors.

Reinstalling operating system or InfoWatch Traffic Monitor system, you will need to install the license anew. Therefore, it is recommended to save license key file to some data storage.

**Warning!**

About license validity check
About license management

Modules and technologies used in product version are listed below.

Interception modules list:

| Subsystem | Event type | Protocol |
|---|---|---|
| TM | Email | POP3<br>IMAP4<br>SMTP<br>NRPC |
| | Web-message | HTTP |
| | Web-mail | HTTP |
| | ICQ | OSCAR |
| | Crawler | - |
| DM | Email | POP3<br>IMAP<br>MAPI<br>SMTP |
| | Email (mobile) | POP3<br>IMAP<br>SMTP |
| | Web message | HTTP<br>HTTPS |
| | Web mail | HTTP<br>HTTPS |
| | Web message (mobile) | HTTP<br>HTTPS |

| Subsystem | Event type | Protocol |
|---|---|---|
| | Web mail (mobile) | HTTP<br>HTTPS |
| | External device | - |
| | Print | - |
| | Skype | SKYPE |
| | XMPP | XMPP |
| | Mail.Ru Agent | MMP |
| | FTP | FTP |
| | SMS | - |
| | Photography | - |
| | WhatsApp | WhatsApp |
| Adapters | MS Lync | SIP |
| | Email (Lotus) | NRPC |
| | External Device (Device Lock) | - |
| | External Device (Lumension Device Control) | - |
| | Print (Device Lock) | - |
| | Print (Lumension Device Control) | - |
| | Web-message (ICAP) | ICAP |
| | Web-mail (ICAP) | ICAP |
| | Cisco UCM Adapter | Push API |

Analysis modules list:

1. Categories and terms;
2. Sample documents detector;
3. Text objects detector;
4. DB unloadings detector;
5. Blanks detector;
6. Graphical objects detector;
7. Stamp detector.

> **Note:**
>
> Technology of leakage challenge blocking on workstations is not licensed according to analysis results.

# Configuring System After Installation

After the System installation the sollowing setting should be configured to provide normal System operating:

- Configuring Time Synchronization - on enabling the authomatical time synchronization on servers;
- Configuring Sphinx in case of distributed installation - on settings for distributed installation;
- Configuring Traffic Interception - settings scecifics for all types of intercepted traffic;
- General Settings - setting procedure to gain the traffic from the managed commutator over SPAN Port technology, interception of a traffic transmitted over ICAP protocol,and system settings for interceptors switching to "in-line" mode sutable for traffic blockage;
- Process Autorun - list of system processes and descriprion of necessity and order of their autorun enabling;
- Configuring OCR Libraries - procedure of installation the packages required for recognizing the text in intercepted events;
- Configuring Email Notifications for Users and Employees - mandatory settings required for support of mail notifications sent as a result of triggering on or another rule in policies (see details in «*InfoWatch Traffic Monitor. User Guide*»);
- Limiting the Number of Found Events - changing maximum number of events displaying in the Management Console;
- Configuring InfoWatch Device Monitor Server - configuring separate modules of Device Monitor Server and editing the logging settings.

# 2.1 Configuring Time Synchronization

1. Set the system time using `date` command. For example, to set 12 August 2013 13:30 run the command with following parameters:
   `date 12081330`
2. Copy system time to configure hardware clock with the command:
   `hwclock --systohc`
3. Check if the system and hardware clock are configured properly:
   `hwclock ; date`
4. The time should be almost the same.
   Stop ntpd service:
   `service iwtm stop ntpd`
5. Define time synchronization server. You can use any exact time service which uses ntp protocol and is available from you network. It can be both network equipment and Windows domain controllers (Active Directory server).
   To check if the server supports NPT use ntpdate -q <IP> command (replace IP by the address of checked server), for example:
   ```
   root@atl-iw:~# ntpdate -q 10.10.0.98

   server 10.10.0.98, stratum 3, offset 9.196765, delay 0.04437

   11 Sep 13:09:02 ntpdate[13819]: step time server 10.10.0.98 offset 9.196765 sec

   root@atl-iw:~#
   ```
6. Configure synchronization by specifying the NTP synchronization server in **/etc/ntp.conf** file. Add entry (replace IP by the actual address of NTP server):
   `server 10.10.0.98`
7. Run ntpd service:
   `service iwtm start ntpd`
8. Check current state of ntpd service with the command:
   `service iwtm status ntpd`
9. Enable automatic time synchronization:
   `chkconfig --level 345 ntpd on`

# 2.2 Configuring Sphinx in case of distributed installation

A full-text query search in Traffic Monitor is performed by means of Sphinx search engine. Service **sphinx** is installed in **All-in-one** or **TME DB server** installation mode (for information on installation modes, see the document "*InfoWatch Traffic Monitor. Installation Guide*", "Installation from TME distribution" article).

A distributed installation is an installation scheme when Traffic Monitor and the database are installed on different servers with keys **TME Node server** and **TME DB server** respectively.

If there are secondary servers, take the following steps:

1. On **TME Node server**, in **web.conf** configuration file, in the `hostname` parameter of the `search` section, specify IP address of the server where the **sphinx** service is running (a server with the database);
2. On **TME DB server**, in **/opt/iw/tm5/etc/serman_resolver.conf** configuration file, in `Host` parameter, specify ID address of the main server.

# 2.3 General settings

The chapter contains information on configuring the System and its components:

- Configuring Server to work with SPAN, or Port Mirroring Technology;
- Intercepting traffic, transmitted via ICAP protocol;
- Configuring Inline Mode for Several Interceptors.

## 2.3.1 Configuring Server to work with SPAN, or Port Mirroring Technology

Traffic is being intercepted from managed switch via SPAN Port technology, or Port Mirroring.

There are different possible deployment schemas:

**Variant 1.** Traffic copy interception and analysis is being performed on one computer (**All-in-one kickstart** key). Cluster is not created:

1. Configure Server to work as Sniffer (see "Configuring Traffic Monitor Server as Sniffer", variant 2)
2. Configure traffic reception parameters from Sniffer (see "Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer").

**Variant 2.** Traffic copy interception and analysis is being performed on different computers, clusterization not used:

1. On one computer (**Node server kickstart** key):
    a. Configure Server to work as Sniffer (see "Configuring Traffic Monitor Server as Sniffer", variant 1).
2. On the other computer (**All-in-one kickstart** key):
    a. Configure traffic reception parameters from Sniffer (see "Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer").

**Variant 3.** Traffic copy interception and analysis is being performed on different computers. To improve performance, create a cluster of two Traffic Monitor server instances:

1. Install and configure Oracle DBMS server (**DB server kickstart** key).
2. On computer, where Sniffer will be running (**Node server kickstart** key):
    a. Configure it to work as Sniffer (see "Configuring Traffic Monitor Server as Sniffer", variant 1).
3. On computer, where Traffic Monitor cluster example will be running (**All-in-one** key):
    a. Configure traffic reception parameters from Sniffer (see "Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer").
    b. Specify clusterization parameters (see "Creating Traffic Monitor cluster").

Repeat i.3 to add one more Traffic Monitor Server example to cluster.

## Configuring Traffic Monitor Server as Sniffer

For Traffic Monitor Server to function as Sniffer, one needs to perform configuration file setup.

In **sniffer.conf** configuration file specify required parameters in sections for each interceptor (sections `Http`, `Icq` and `Smtp`):

| Parameter | Description |
|---|---|
| `Interface` | The network interface used to transfer data from the switch |
| `OpenInSec` (subsection `Timeouts`) | Time to keep connection alive (in seconds) if no packages are transmitted. The recommended value – `600`. |
| `LiveInSec` (subsection `Timeouts`) | Timeout (in seconds) when the status of connection must change to *ESTABLISHED*. If the status is not changed, connection will be automatically terminated. Recommended value – `86400`. |
| `CloseInSec` (subsection `Timeouts`) | Time to keep the connection alive (in seconds) when the status is changed to *TIME_WAIT*. The recommended value – `300` |
| `TailInSec` (subsection `Timeouts`) | Wait time for sent packages (in seconds) after connection has been terminated |
| `QueueMemorySizeInBytes` | The size of memory (in bytes), which is used to receive packages. When the channel utilization is high, you can increase this value. The range of values: from 1 to 500 Mb The recommended value – `16777216` |

1. Stop server processes of Traffic Monitor:
   `service iwtm stop`
2. Configure process autostart:

- Variant 1. Traffic copy interception and analysis is being performed on different computers.
  Configured Traffic Monitor Server example will be configured only as Sniffer (traffic interception):
  a. Enable **iw_sniffer** process autostart.
  b. Disable other processes autostart.

> **Note:**
>
> For more information on enabling and disabling autostart see "Enabling and disabling autorun processes".

- Variant 2. Traffic copy interception and analysis is being performed on one computer. Traffic Monitor Server will receive traffic copy from switch (Sniffer function), analyze received data and upload it to database (Traffic Monitor Server function):
  a. Enable **iw_sniffer, iw_loader, iw_updater, iw_warpd** and **iw_adlibitum** processes autostart.
  b. Disable other processes autostart.

> **Note:**
>
> For more information on enabling and disabling autostart see "Enabling and disabling autorun processes"

3. In **/opt/iw/tm5/etc/sniffer.conf** file, section `Iscp`, configure traffic interception parameters:
   - `ListenHost`. IP-address for incoming connections.
   - `ListenPort`. Port for incoming connections.
4. Start Traffic Monitor processes:
   `service iwtm start`

## Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer

Configuration is performed on the computer where Traffic Monitor Server is installed. Configuring these settings is required if Sniffer and Traffic Monitor Server are installed on the same computer.

Go to `/opt/iw/tm5/etc` directory configure the following settings:

1. In **proxy.conf** configuration file, located in `/opt/iw/tm5/etc` directory, `Startup` section, enable autostart for required traffic interceptors (setup for SMTP-,HTTP(S), ICQ traffic:
   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – enabling all interceptors;
   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – enabling **iw_proxy_http** interceptor;

- `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – disabling all interceptors.

> **Note:**
>
> For NRPC traffic interceptor autostart configuration description, see "SPAN, или Port Mirroring".

2. Make sure **proxy.conf** configuration file has `false` meaning for SkipNegotiate parameter.
3. In case you need to intercept ICQ traffic, which should be transmitted via proxy-server (over HTTP), set true value for `IcqFilter` parameter in **proxy.conf** configuration file.
4. In **proxy.conf** configuration file, in `Iscp` part of sections `Smtp, Icq, Http` create values of `Host` and `Port` parameters..
   For example,
   To configure interaction with computer, which has 10.20.30.40 IP-address and port 1234, `Iscp` section for ICQ interceptor will look as follows:

```
"iscp": {
"ListenArea": "icq",
"Host": 10.20.30.40,
"Port": 1234
}
```

## Creating Traffic Monitor cluster

Intercepting traffic copy via Sniffer, to increase System productivity, one can create Traffic Monitor server clusters.

> **Warning!**
>
> One cluster can contain up to two Traffic Monitor Server examples. It is not recommended to use more than 3 clusters.
>
> Using clusters, network connection between Sniffer and Traffic Monitor server should provide transmission speed twice as large as the speed at which traffic arrives at Sniffer.

To create Traffic Monitor servers cluster, create clusterization configuration parameters in **/opt/iw/tm5/etc/sniffer.conf** configuration file on each server:

1. Make sure that `Usedareas` section looks as follows:
   ```
   "UsedAreas": [
   "capstack",
   "http",
   ```

```
"icq",
"smtp"
]
```

This setting is by default.

2. In **proxy.conf** configuration file, in `Iscp` part of sections `Smtp`, `Icq`, `Http` create values of `Host` and `Port` parameters.
   For example,
   To set up interaction with computer having 10.20.30.40 IP address and **1234** port, Iscp part for ICQ interceptor will look as follows:

```
"iscp": {
"ListenArea": "icq",
"Host": 10.20.30.40,
"Port": 1234
}
```

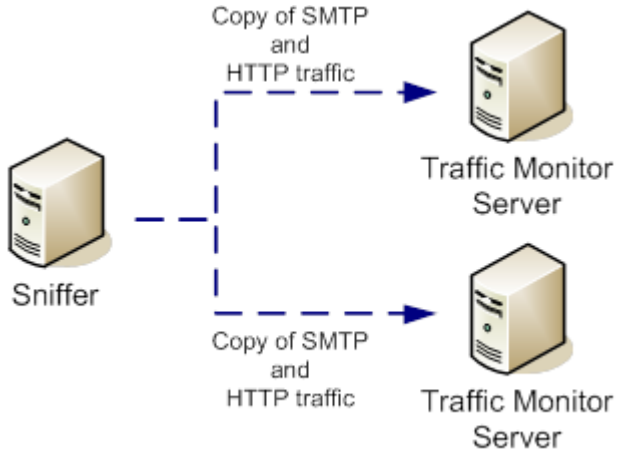
3. In **sniffer.conf** configuration file create Balancer value for each of Smtp, Icq, Http sections. Possible values:

- `Easy`. For each new TCP connection an instance of Traffic Monitor Server is being chosen with **iw_proxy**. Thus, alternately all Traffic Monitor Server instances are used.
- `IpPref`. The distribution of traffic across multiple server instances of Traffic Monitor with **iw_proxy** is based on the IP-address of the client. This means, that the data with identical client IP address will be transmitted to one Traffic Monitor instance.

By default IpPref parameter is used.

**Example. Creating a cluster of two Traffic Monitor server instances**

The system captures a copy of SMTP- and HTTP-traffic via Sniffer. To improve performance analyzing the traffic a cluster of two Traffic Monitor Server is being created (see pic. 3).




Picture 3. Creating a cluster of two Traffic Monitor Server instances

### 2.3.2 Intercepting traffic, transmitted via ICAP protocol

A proxy supporting ICAP intercepts HTTP traffic and delivers it to Traffic Monitor server for analysis and uploading to the database.

> **Note:**
>
> If you use Blue Coat as proxy server, HTTPS traffic can also be intercepted. In this case, the Blue Coat proxy must be configured to process HTTPS traffic and send it to Traffic Monitor server as HTTP traffic.

The scheme supports user data processing with the following methods of authentication: NTLM, LDAP, Basic, Digest.

In this scheme, Traffic Monitor server IW ICAP module is being automatically installed.

> **Warning!**
>
> Traffic Monitor Server and proxy with ICAP client must be located in the same subnetwork.
>
> The web-browser of each workstation must be configured to use the required proxy server (SQUID, Blue Coat, Cisco IronPort) for HTTP(S) traffic. For more information on configuring the settings, see the documentation for your web-browser.

A proxy supporting ICAP intercepts HTTP traffic and delivers it to Traffic Monitor server for analysis and uploading to the database.

Depending on transmission type (Copy or Block), the following variants of HTTP traffic are possible:

- Copy type – copy of HTTP traffic is transmitted to TM Server for analysis; traffic is transmitted via proxy-server to the next chain link, depending on corporate infrastructure.
- Block type – HTTP traffic is analyzed by Traffic Monitor system. Depending on the fact if there is violation or not, the following routes of traffic are possible:
  - In case there is no violation, a message which allows traffic transmission is returned to a proxy server. From the proxy-server, traffic is forwarded to the next link in a chain, depending on corporate infrastructure;
  - In case there is a violation, a message which prohibits traffic transmission is returned to a proxy-server. Traffic is blocked and the user, who sent the traffic, gets a warning message.

> **Note:**
>
> The text of the error message is contained in the error.html file which is located in the `/opt/iw/tm5/etc` directory.

In this chapter:

- Configuring ICAP;
- Configuring Blue Coat SG Series as an ICAP-client;
- Configuring SQUID as an ICAP-client;
- Configuring Cisco Iron Port as an ICAP-client;
- Configuring McAfee Web Gateway as an ICAP-client.

## Configuring ICAP

IW ICAP module is being automatically installed along with Traffic Monitor server (**IWTMX**, **IWALLX** or **IWTMSX** keys). **iw_icap** process autorun is being on TM Server is being enabled by default.

HTTP- and HTTPS- traffic interception is performed by same means of the System but configuration of side tools is different (see below).

To provide HTTP(S)- traffic interception via ICAP protocol, it is necessary to configure HTTP- and HTTPS-interception parameters on proxy-server.

> **Warning**
>
> The web-browser of each workstation must be configured to use the required proxy server (SQUID, Blue Coat) for HTTP(S) traffic. For more information on configuring the settings, see the documentation for your web-browser.

In **system.lua** configuration file, located in `/opt/iw/tm5/etc/scripts` directory, define code section: Configure transport mode for traffic transmitted via ICAP.

**For traffic to be transmitted in «Copy» mode**:

1. `if not get_child(processing, 'transport_mode') then processing:add_child('transport_mode'):set_text('Copy');`
2. In **icap.conf** configuration file, located in `/opt/iw/tm5/etc/` directory, specify true value for `AsyncCheck` parameter of `Icap` section.

**For traffic to be transmitted in «Block» mode**:

1. In **system.lua** configuration file, located in `/opt/iw/tm5/etc/scripts` directory, define code section:
   `if not get_child(processing, 'transport_mode') then processing:add_child('transport_mode'):set_text('Normal');`
2. In **icap.conf** configuration file, located in `/opt/iw/tm5/etc/` directory, specify false value for `AsyncCheck` parameter of `Icap` section.

> **Warning!**
>
> Mode, configured in system.lua will be applied to SMTP- and HTTP(S) interceptors. To perform finer tune, see "Configuring Inline Mode for Several Interceptors".

Configure HTTP- and HTTPS- interception parameters on proxy-server.

> **Note:**
>
> This setting depends on proxy-server configuration. You can find actual information on configuration from proxy-server documentation.
>
> If necessary, use Blue Coat SG Series setup recommendations (see "Configuring Blue Coat SG Series as an ICAP-client") and SQUID (see "Configuring SQUID as an ICAP-client").

## Configuring Blue Coat SG Series as an ICAP-client

The proxy-server should have using ICAP in Request Mode allowed and parameters of interaction with Traffic Monitor configured. These settings are performed via Web-interface, under administrator user account.

> **Note:**
>
> The configuration procedure described below may vary depending on the proxy server's version and model.
>
> To intercept the HTTPS traffic, it is necessary to implement ssl-inspection (ssl-bump) on the proxy server. For more information, see documentation for your proxy server.

1. Go to the **Configuration** tab.
2. Go to the **External Services ► ICAP** section. Create the **tm** service. Configure the settings of the service:
   **Service URL**: `icap://<TM_server_IP>/reqmod`
   Example: `icap://10.60.0.20/reqmod`.
   **Maximum number of connections:** `10`
   **Connection timeout:** `70`
   Check **This service supports plain ICAP connection**. In Plain ICAP port field, specify **1344**.

   > **Warning!**
   >
   > The value of **Plain ICAP port** field must match the value of `ListenPort` setting in **/opt/iw/tm5/etc/icap.conf** file, Icap section. If another value was set for `ListenPort` setting, you need to adjust it.

   On **ICAP v1.0 Options** panel, configure the following settings:
   **Method supported:** select request modification
   **Send:** Check Authenticated User, Client address and Server address boxes.

3. Go to the **Health Checks ► General** section. Make sure that verification of server status is enabled — **Health Checks** tab displays the addresses:
   `icap.tm`
4. To check availability of all servers listed click **Perform health check** button.

## Recommendations on SQUID configuration

Documentation contains information on configuring SQUID proxy server for MS AD user authentication, SSL interception (ssl-bump) and traffic verification via ICAP.

In this chapter:

- SQUID installation;
- Configuring ICAP;
- Configuring SSL interception and disclosure;
- Configuring user authentication.

## SQUID installation

Before installing SQUID proxy server, you need to:

- download an RMP package or an archive (that should be then unpacked) from a repository or from CD/DVD;
- make sure that the PC on which SQUID will run has access to the external network and users who will use this proxy server have access to this PC.

**To install an RMP package of SQUID proxy server, log into the System under `root` and enter the following command:**

```
rpm -i squid-3.4.0.2-2.el6.x86_64.rpm
```

**If the package is installed successfully, the following information will be displayed:**

```
Preparing...    ################  [100%]
1:squid         ################  [100%]
```

**To access the configuration file, enter:**

```
cd /etc/squid/
vim squid.conf
```

## Configuring ICAP

**To configure ICAP, add ICAP processing line to the end of squid.conf**:

```
icap_enable on
icap_service service_req reqmod_precache bypass=1 icap://10.60.7.7:1344/request
adaptation_access service_req allow all
icap_send_client_ip on
icap_send_client_username on
```

## Configuring SSL interception and disclosure

SSL-Bump mode is being used for HTTPS sessions encrypted content interception. SQUID performs SSL-connection with server and receives its certificate as first intercepted HTTP request is transmitted. After that SQUID uses host name from real, received from server certificate and creates fictitious certificate whereby simulates requested server in interaction with client, wherein proceeding on using SSL connection. Except for HTTPS connections, specified scheme can be used to intercept major HTTP requests.

1. Create catalogue to store SQUID certificates and change its rights so that user **squid** is an owner of its content:
   ```
   cd /etc/squid
   mkdir ssl_cert
   chown -R squid:squid /etc/squid/ssl_cert/
   ```
2. Generate root certificate for browser of workstations traffic from which will be intercepted.
3. Move file with extention **.der** to Windows machine and install it as trusted certificate to computer storage:
   ```
   openssl req -new -newkey rsa:1024 -days 720 -nodes -x509 -keyout /etc/squid/ssl_cert
   /IW.pem -out
   /etc/squid/ssl_cert/IW.pem
   openssl x509 -in /etc/squid/ssl_cert/IW.pem -outform DER -out /etc/squid/ssl_cert/IW.
   der
   ```
4. Create database for substitute certificates and create user **squid** its owner:
   ```
   /usr/lib64/squid/ssl_crtd -c -s /var/lib/ssl_db/
   chown -R squid:squid /etc/squid/ssl_cert/
   squid -k reconfigure
   ```
5. In configuration file **squid.conf** Comment out the setting `http_port` and add the following lines:
   ```
   #http_port 3128
   http_port 3128 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB
   cert=/etc/squid/ssl_cert/IW.pem
   sslproxy_flags DONT_VERIFY_PEER
   sslproxy_cert_error allow all
   sslproxy_cert_error allow all
   ssl_bump client-first all
   ssl_bump client-first all
   ssl_bump none all
   sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/ssl_db -M 4MB
   ```
6. Check configuration and restart server **squid**:
   ```
   squid -k reconfigure
   service squid restart
   ```
7. Configure browser to user new proxy server.

## Configuring user authentication

SQUID authentication service is intended to decode HTTP `Authorization` header and transmit decoded information to a third-party module. User access is being provided in case information is correct. When information is incorrect or missing, SQUID returns 407 error to the client. Thus, all the work on user authentication is being performed by third-party modules. Location of these modules depends on SQUID distribution. For example, in Debian+SQUID3 they are located in catalogue:`/usr /lib/squid3`, in Red Hat they are likely to be located in `/usr/lib/squid`. To see what authentication methods, third-part modules placement and other parameters are supported by SQUID, use command `squid3 -v`:

```
squid -v
Squid Cache: Version 3.4.0.2
configure options: '--host=x86_64-redhat-linux-gnu' '--build=x86_64-redhat-linux-gnu' '--
program-prefix='
'--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--
sysconfdir=/etc' '--datadir=/usr/share'
'--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--
sharedstatedir=/var/lib'
'--mandir=/usr/share/man' '--infodir=/usr/share/info' '--exec_prefix=/usr' '--libexecdir=
/usr/lib64/squid'
'--localstatedir=/var' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid'
'--with-logdir= of $ (localstatedir)/log/squid' '--with-pidfile= of $ (localstatedir)/run
/squid.pid'
'--disable-dependency-tracking' '--enable-eui' '--enable-follow-x-forwarded-for' '--
enable-auth'
'--The enable-auth-basic=DB, the LDAP, MSNT, MSNT-multi-domain, NCSA, NIS, PAM, the POP3,
the RADIUS, SASL, SMB, getp
wnam '--enable-auth-ntlm=smb_lm,fake' enable-auth-digest=file, LDAP, eDirectory
'--enable-auth-negotiate=kerberos,wrapper'
'--enable-external-acl-helpers=wbinfo_group,kerberos_ldap_group,AD_group' '--enable-cache-
digests'
'--enable-cachemgr-hostname=localhost' '--enable-delay-pools' '--enable-epoll' '--enable-
icap-client'
'--enable-ident-lookups' '--enable-linux-netfilter' '--enable-removal-policies=heap,lru'
'--enable-snmp'
'--enable-ssl' '--enable-ssl-crtd' '--enable-storeio=aufs,diskd,ufs,rock' '--enable-
wccpv2' '--enable-esi'
'--with-aio' '--with-default-user=squid' '--with-filedescriptors=16384' '--with-dl' '--
with-openssl' '--with-pthreads'
'--disable-arch-native' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-
linux-gnu'
'CFLAGS= is O2 -g' 'CXXFLAGS= is O2 -g -fPIC'
'PKG_CONFIG_PATH=/usr/lib64/pkgconfig:/usr/share/pkgconfig'
```

Third-party modules interaction and settings description is being performed with the help of `auth_param` parameter. Client will alternately attempt to use authentication schemes in the order they have been set in **squid.conf**. Newly configured authentication scheme enters into force after squid service restart. To change existing schemes without service restart, use `squid3 -k reconfigure` or `/etc/init.d /squid3 reload` commands.

To control internet access, create acl, which will use configured authentication module. To do this, acl in `selection_type` field must have `proxy_auth`, `proxy_auth_regex` or `external` value using `%LOGIN` variable. Set access permission in`http_access` parameter for specified acl. Below the format is listed, which specifies the type of used authentication (format of using `auth_param` parameter):
`auth_param authentication_scheme schem_parameters [parameters_value]`

## Configuring Cisco Iron Port as an ICAP-client

To configure Cisco Iron Port as an ICAP-client:

- Add Traffic Monitor as an external DLP server
- Create and configure external DLP policy

**To add external DLP server:**

1. In browser open Cisco IronPort management console:
   `https://<Cisco IronPort hostname or IP-address>:8443`
2. Go to **Network > External DLP Servers** tab.
3. In the opened windows press **Edit Settings** button.
   
4. Fill in the fields in accordance with the table:

| Parameter | Value |
|---|---|
| External DLP Servers | The following fields concerning external server of outgoing traffic filtering should be filled in:<br>• **Server address and port**. Domain machine name and port used by Traffic Monitor ICAP-server<br>• **Reconnection attempts**. Number of reconnection attempts with Traffic Monitor ICAP-server. Recommended value is `5`.<br>• **DLP Service URL.** Traffic Monitor ICAP-server URL.<br>URL should start with `icap://`. Example: `icap://FQDN:1344/reqmod` |
| Load Balancing | Load balancing. In case one Traffic Monitor ICAP-server is used for traffic filtering, `Fewest Connections` value should be specified. |
| Service Request Timeout | Timeout used for Cisco IronPort to wait for reply from Traffic Monitor ICAP-server. Default value is `60 seconds`. |
| | Maximum number of simultaneous connections.<br>Do not change default `25` value. |

| Parameter | Value |
| --- | --- |
| Maximum Simultaneous Connections | |
| Failure Handling | Parameter, which allows to set Cisco IronPort behavior in case Traffic Monitor ICAP-server is unavailable. Recommended value is Permit all data transfers to proceed without scanning. |

5. Press **Add Row** to create additional ICAP-server.
6. Press **Submit** to save changes.
7. Press **Start Test** to check connection with ICAP-server.

### To create external DLP policy:

1. Go to **Web Security Manager** section.
2. Press **Add Policy** button.
3. Type in the name of the policy in **Policy Name** field (for example, TM ICAP)
4. In **Identities and Users** section choose users or user group, controlled by this policy.
5. Press **Advanced** and choose HTTP in **Protocols** field.
6. Save changes.

### To configure external DLP policy:

1. Go to **Web Security Manager** section:



2. Choose policy in **Destinations** column.
3. In **Edit Destination Settings** drop-down list choose **Define Destinations Scanning Custom Settings** value.
4. In **Destinations to scan** choose **Scan All Uploads**.
5. Press **Submit** to save the changes.

**Note:**

Cisco IronPort can as well analyse HTTPS-traffic. In this case certificate replacement takes place. HTTPS-traffic is being decrypted and processed as HTTP. Interaction between Cisco IronPort and Traffic Monitor does not change. Find additional information on HTTPS decryption in Cisco IronPort documentation (see chapter «Decryption Policies»).

## Configuring McAfee Web Gateway as an ICAP-client

1. Enter McAfee Web Gateway web-console.
2. Go to **Rule Sets** tab of **Policy** section.
3. Press **Add** and choose **Rule Set From Library**.
4. In the opened window choose **ICAP Client** library, press **OK**.
   In **Rule Sets Library** list **ICAP Client** rules will be added.
5. Open **ICAP Client** list and mark **ReqMod** rule.
6. In the working area on the right from the rules list press **Show details** button.
7. Tick **Enabled** attribute in **DLP Solution: Skip Requests That Do Not Carry Information** line.
8. Use **ReqMod** link in **Call ReqMod Server** line.
9. In the opened window, on **Edit Settings** tab**, Settings content** section, press **Edit**.
10. Enter server data so that it looks as follows:

11. Press **OK**.
12. In the opened window press **OK**.
13. Open **ICAP Client** list and choose **RespMod** rule.
14. Use **RespMode** link in **Call RespMod Server** line.
15. In the opened window, on **Edit Settings** tab**, Settings content** section, press **Edit**.
16. Repeat step 10 specifying **respmod** in **URI** field.
17. Press **OK**.
18. In the working area on the right from the rules list, untick **Enable** attribute**.**

    **Note:**

    Last step is required so that user changes are not being blocked from saving by server.

19. Press  several times to move **ICAP Client** set of rules on the top of the list.
20. Press  button in the top left corner of the browser.

## Disabling ICAP

In case HTTP/HTTPS requests interception over ICAP is no longer required, you can disable module **iw_icap**.

**To disable iw_icap module:**

1. Stop Traffic Monitor processes:
   `service iwtm stop`
   Disable process autostart `iw_icap` (see "Enabling and disabling autostart of processes").
2. Start Traffic Monitor processes:
   `service iwtm start`
3. Check state of Traffic Monitor processes:
   `service iwtm status`

After disabling module, return original settings of proxy server.

### 2.3.3 Configuring Inline Mode for Several Interceptors

In case system uses inline mode for SMTP- and HTTP(S)-traffic, than you need to change **system.lua** configuration file in a following way..

1. Enter the system under **root** user:
   `su - root`
2. Open **system.lua** file, located in `/opt/iw/tm5/etc/scripts` directory, to edit.
3. Change code section
   ```
   if not get_child(processing, 'transport_mode') then
   processing:add_child('transport_mode'):set_text('Copy');
   end;
   ```
   to the next one:
   ```
   if not get_child(processing, 'transport_mode') then
   local monitor = get_monitor(root);
   if monitor == 'SMTP' then
   processing:add_child('transport_mode'):set_text('Normal');
   elseif monitor == 'HTTP' then
   processing:add_child('transport_mode'):set_text('Normal');
   else
   processing:add_child('transport_mode'):set_text('Copy');
   end
   end;
   ```
4. Depending on regime you want to enable for an interceptor, specify:
   **For SMTP interceptor**

- To use «Copy» type:
  if monitor == 'SMTP' then
  processing:add_child('transport_mode'):set_text('Copy');
- To use «Block» type:
  ```
  if monitor == 'SMTP' then
  processing:add_child('transport_mode'):set_text('Normal');
  ```

  **For HTTP(S)-interceptor**

- To use «Copy» type:
  if monitor == 'HTTP' then
  processing:add_child('transport_mode'):set_text('Copy');
- To use «Block» type:
  ```
  if monitor == 'HTTP' then
  processing:add_child('transport_mode'):set_text('Normal');
  ```

1. Save file.

> **Warning!**
>
> Configuring HTTP, it is also required to edit **icap.conf** according to the chosen mode (see "Configuring ICAP ".)

2. Reboot the system:
   ```
   service iwtm restart
   ```

# 2.4 Configuring traffic interception

System can perform data interception, using the following protocols.

| Protocol | Description |
|---|---|
| SMTP (Simple Mail Transfer Protocol) | Mailing protocol, which is used by mailing client to send outgoing email messages to server.<br>It works in tandem with the POP3 protocol. |
| POP3 (Post Office Protocol, version 3) | Mail protocol, which is used by mail client to recieve incoming email messages from server.<br>To send emails SMTP protocol is used. |
| HTTP (HyperText Transfer Protocol) | Data transfer protocol based on «client-server» technology, which is used to recive text information, strem video and sound from the web-site. You can realize interception of all transmitted data in the Internet (visited pages, portals, recived and sent emails and messages). |
| HTTP(S) | HTTP protocol extention, which supports encryption. Data, transmitted over HTTP, are packed into cryptographic protocol, thereby providing data protection. |

| Protocol | Description |
|---|---|
| ICQ (OSCAR) | Instant and offline text messaging protocol, used by ICQ, AIM, Miranda, QIP programs. You can perform text messages interception, transmitted via these instant messaging programs. |
| NRPC | Mail Transfer Protocol in IBM Notes. |
| IMAP4 (Internet Mail Access Protocol) | Protocol of access to email. In accordance with POP3 protocol, it is used for work with emails, but provides more broad work capabilities to work with mailbox. For example, access to processing events, located on server, as if they were located on local reciever computer, without necessity of permanent file transfer with content from server and back. SMTP protocol is used to send messages. You can perform incoming emails interception, transmitted by e-mail clients. |

Depending on intercepted traffic type system can be configured as follows:

- Configuring SMTP Traffic Interception;
- Configuring POP3 Traffic Interception;
- Configuring HTTP Traffic Interception;
- Configuring HTTPS Traffic Interception;
- Configuring NRPC Traffic Interception;
- Configuring IMAP4 Traffic Interception;
- Recieving Objects Intercepted by InfoWatch Device Monitor;
- Revision of Files from the Corporate Network.

**Warning!**

It is assumed, that System is already installed before configuration starts.

Find more information on installation for each deployment schema in document "InfoWatch Traffic Monitor. Installation Guide".

**Warning!**

After traffic interception setup completion, it is necessary to configure object analysis parameters (see document "InfoWatch Traffic Monitor. User Guide").

## 2.4.1 Configuring SMTP Traffic Interception

Chapter contains information on how to configure SMTP traffic interception using the following technologies:

- SPAN, or Port Mirroring;

- Recieving Copies from Mail Server;
- Inline Mode;
- Configuring Mail Servers for SMTP Traffic Interception.

Detailed information SMTP traffic interception scheme is available in article "SMTP Traffic Interception Scheme".

## SPAN, or Port Mirroring

1. Configure server (servers) for working with SPAN, or Port Mirroring (see "Configuring Server to work with SPAN, or Port Mirroring Technology").
2. Make sure, that **proxy.conf** configuration file, which is located in `/ort/iw/tm5/etc`, in section `Startup` SMTP traffic autostart is enabled:
   ```
   "Startup": {
   "Enabled": true,
   "smtp": true
   ```
3. Make sure, that autostart of all processes, which participate in mail interception and analysis, is enabled:
   **iw_sniffer**, **iw_proxy_smtp**, **iw_messed**, **iw_warpd**, **iw_cas**, **iw_loader** (see "Enabling and disabling autorun processes").
4. To avoid dublication of intercepted data, disable **iw_smtpd** process (see "Enabling and disabling autorun processes").

## Recieving Copies from Mail Server

A rule for sending a shadow copy (BCC) of each sent message should be configured on a corporate mail server. The copy is sent to a nonexistent mail address with domain whose IP-address corresponds to Traffic Monitor Server. This functionality is supported by most mail servers.

Integration of Traffic Monitor Server with a mail server is performed the following way. Postfix mail server which is embedded in the Traffic Monitor system receives copies of messages sent via SMTP. Copies are delivered to the port **25** and transmitted to the **iw_smtpd** process on port **2025**. An event for each message is created in the System. Information about those events is then placed to a database.

To configure receiving copies from a mail server, do the following steps:

1. Make sure, that **iw_smtpd** process autostart is enabled (see "Process Autorun")
2. On a mail server, configure SMTP-messages shadow copy forwarding (BCC - Blind Carbon Copy) to Traffic Monitor Server. Find setup example for Microsoft Exchange Server 2007 and 2010 in "Forwarding BCC with Microsoft Exchange Server 2007 and 2010".
3. Configure embedded Postfix server (see "Configuring Postfix Server embedded in Traffic Monitor system").

4. Make sure, that autostart of all processes, which participate in traffic interception and analysis, is enabled:
   **postfix, iw_smtpd, iw_messed, iw_warpd, iw_cas, iw_loader** (see "Process Autorun").
5. Make sure that in the system.lua configuration file which is located in `/opt/iw/tm5/etc/scripts` directory, the value of the `set_text` parameter is `Copy`:

```
if not get_child(processing, 'transport_mode') then
processing:add_child('transport_mode'):set_text('Copy');
```

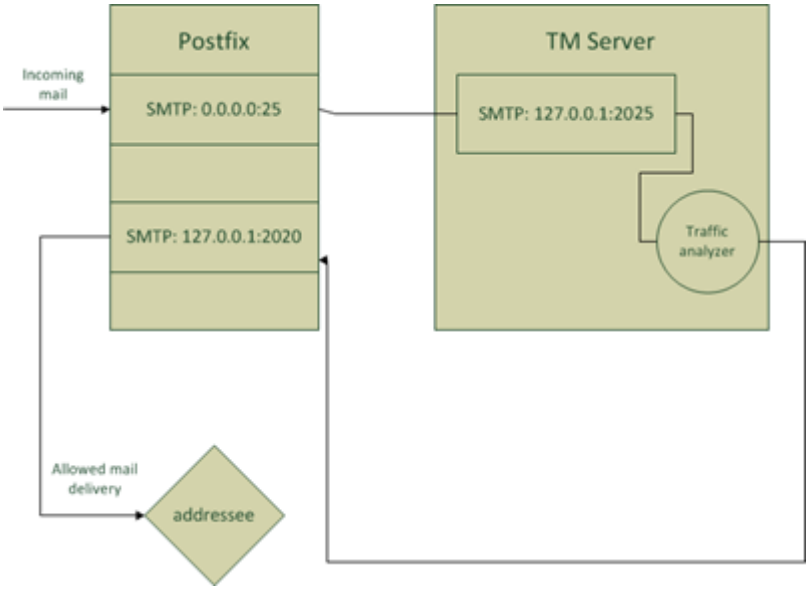
> **Warning!**
>
> Chosen mode will be applied to SMTP and HTTP(S) interceptors. For more flexible configuration see "Configuring Inline Mode for Several Interceptors".

## Inline Mode

Traffic Monitor Server is used as an intermediate mail server. It includes Postfix mail server.

Integration of Traffic Monitor mail server with a mail server in implemented the following way. Postfix mail server which is embedded in the Traffic Monitor system receives incoming SMTP messages via port **25**. SMTP messages are then transmitted to the **iw_smtpd** process via port **2025**. An event for each message is created in the System. Depending on the selected scheme (Copy or Block), the following types of SMTP traffic transmission are possible:

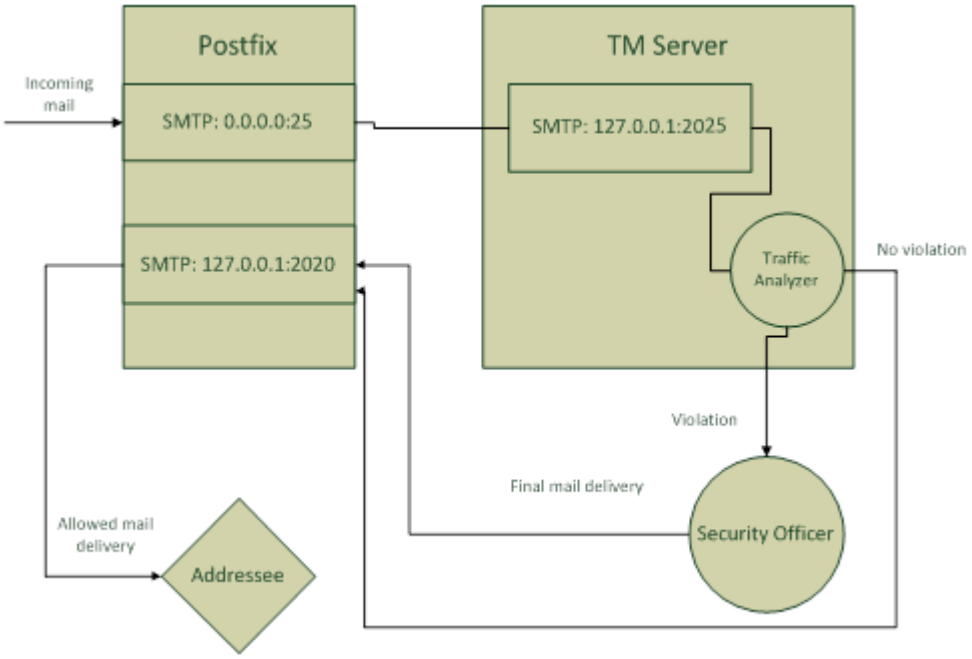
- Copy type – SMTP traffic is transmitted to recipient via Postfix or to the next relay-server in the corporate mailing System.




Picture 1. Postfix integration (Copy)

- Block type – SMTP traffic is analyzed by Traffic Monitor System, and

- In case there is no violation, SMTP traffic is transmitted to the recipient or to the next relay-server in the corporate mailing System via the embedded Postfix server. Delivery is performed as follows: iw_messed process transmits messages to **2020** port of Postfix mail server. Postfix mail server delivers messages to recipients directly or transmits them to the next relay-server;
- In case there is a violation, System blocks delivery of the message. The message will be delivered only if a Security Officer allows delivery in Management Console (see document «*InfoWatch Traffic Monitor. User guide*»). Delivery is performed as follows: **iw_messed** process transmits messages to **2020** port of the embedded Postfix mail server. Postfix mail server delivers messages to recipients directly or transmits them to the next relay-server;




Picture 2. Postfix integration (Block)

**To configure inline mode, follow the steps:**

1. Configure Traffic Monitor as a relay-server on a corporate mail server.

> **Note:**
>
> If more than one mail server are used in the organization, each of them should be configured to send outgoing messages to Postfix server.
>
> Configuration process can be different depending on the mail server used in the company.

As a result, all mail traffic sent from a corporate mail server will be transmitted to Traffic Monitor Server.

2. Make sure that autostart for the **iw_smtpd** and **iw_deliver** processes has been enabled (see "Process Autorun").
3. Configure Postfix server which is embedded in the System (see "Configuring Postfix Server in Traffic Monitor system").
4. In the **system.lua** configuration file, which is located in the **/opt/iw/tm5/etc/scripts** directory, enter the code section for the selected mode:
   - If Copy mode is used:

```
if not get_child(processing, 'transport_mode') then
processing:add_child('transport_mode'):set_text('Copy');
```

   - If Block mode is used:

```
if not get_child(processing, 'transport_mode') then
  processing:add_child('transport_mode'):set_text('Normal');
```

> **Warning!**
>
> Chosen mode will be applied to SMTP and HTTP(S) interceptors. For more flexible configuration see "Configuring Inline Mode for Server Interceptors".

## Configuring Mail Servers for SMTP Traffic Interception

Chapter contains information on configuring mail servers to intercept SMTP traffic with Traffic Monitor:

- Forwarding BCC with Microsoft Exchange Server 2007 and 2010;
- Configuring BCC with ZCS Zimbra;
- Forwarding BCC with MDaemon;
- Configuring Postfix server in Traffic Monitor System.

## Forwarding BCC with Microsoft Exchange Server 2007 and 2010

> **Warning!**
>
> In this chapter you will find guidance for SMTP-messages shadow copy transmission (BCC – Blind Carbon Copy) to Traffic Monitor Server when Microsoft Exchange Server 2007 or 2010 is used. For other mail servers, configuration process may differ.

To enable sending shadow copies of SMTP messages, a connector for sending messages to Traffic Monitor Server should be created and configured in the Exchange Management Console. For this, perform the steps below.

**Creating SMTP connector that will send message copies to Traffic Monitor Server**

1. Choose **Organization Configuration –> Hub Transport** node and press **New Send Connector**.
2. In the window of Connector creation wizard, type in connector name and choose **Custom** type from the drop-down list. Click **Next**.
3. At the **Address space** step, create a new address space to transmit traffic. To do this, press **Add**. In the dialog box that opens, specify address space parameters and press **OK**. Then click **Next**.
4. At the **Network Settings** step, choose **Route mail through the following smart hosts** and press **Add**. In the opened dialog box, specify IP-address of Traffic Monitor server, to which mail will be transmitted and press **OK**. Then click **Next**.
5. At the **Configure smart host authentication settings** step, choose **None**: by default Postfix does not require authorization on the Traffic Monitor Server. Click **Next**.
6. At the **Source Server** step, choose a server, the connector will be located on. Click **Next**.
7. At the **New Connector** step make sure, that connector parameters have been specified correctly, and click **New**. Wait for the creation process to be completed and click **Finish**.

The window of Connector creation wizard will be closed.

**Creating contact to which message copies will be sent**

1. Choose **Recipient Configuration –> Mail Contact** node and press **New Mail Contact**.
2. In the window of Contact creation wizard, choose **Mail Contact** and click **Next**.
3. At the **Configure smart host authentication settings** step, type in information about contact. In the **External e-mail address** line, press **Edit**. In the opened **SMTP Address** dialog box, type in mail address, which will receive message copies.

   > **Warning!**
   >
   > Mail contact domain should match the connector domain.

4. At the **New Mail Contact** step, make sure that connector parameters are specified correctly, and click **New**. Wait for process completion and click **Finish**.

The window of Contact creation wizard will be closed.

> **Warning!**
>
> For the System to function properly, it is necessary to have OS Linux user with the same domain name as a new contact.
>
> For example, if *user@company.com* contact is created, it is necessary that *user* should be among Linux clients.
>
> To add a user on OS Linux, issue the following command under root:

useradd <username>

where <username> is a required user name. In the example above, issue the following command:

useradd user

**Creating transport rule for copying messages**

1. Choose **Organization Configuration -> Hub Transport** node and press  **New Transport Rule**.
2. In the Transport rule creation wizard, type in a name of the rule being created and set a flag in the **Enable Rule** field. Click **Next**.
3. At the **Conditions**, select the **from users inside or outside the organization** check box. As a condition parameter, choose **Inside**. Click **Next**.
4. At the **Actions** step, select the **Blind carbon copy (Bcc) the message to address** checkbox. In the dialog box that opens, click the link with **address** parameter and in the **Select Recipient** window, choose created contact. Click **OK**. In the wizard window, click **Next**.
5. You can configure exceptions at the **Exceptions** step if necessary. For example, for the messages from particular users not to be copied, select the **except when the message is from people** checkbox and choose desired users in the exception parameters. Click **Next**.
6. At the **Create Rule** step, make sure, that parameters have been specified correctly, and press **New**. Wait for the creation process to be completed and click **Finish**.

**Blocking mail delivery when Traffic Monitor Server in not available**

1. Choose **Organization Configuration -> Hub Transport** node and press  **New remote Domain** .
2. Specify the same name as the domain name used in item 3 step 2 of this chapter (creating contact, to which message copies will be sent).
3. Right-click on the new domain and choose **Properties** from the context menu.
4. In the window that opens, go to the **Message Format** tab.
5. Deselect the **Allow non-delivery reports** check box.
6. Click **OK**.

## Configuring BCC with ZCS Zimbra

**Warning!**

All commands should be executed under **zimbra** user.

**Configuring transport table**

Use configuration block for Zimbra 5.0.9 or higher with the following string:

```
zmlocalconfig -e postfix_transport_maps="hash:/opt/zimbra/postfix/conf/transportfile
proxy:ldap:/opt/zimbra/conf/ldap-transport.cf"
```

> **Warning!**
>
> This command should be executed using **zmlocalconfig**. Editing **main.cf** will not be sufficient in the situation.

1. Check the existing transport table:
   `zmlocalconfig grep -i postfix_transport_maps`
   Get the command output of the following form:
   `postfix_transport_maps = proxy:ldap:/opt/zimbra/conf/ldap-transport.cf`
2. Create transport file:
   `mcedit /opt/zimbra/postfix/conf/infowatch`
3. Add the following line to file:
   `dlp.iw :[192.168.0.144]`
4. Check rights (**zimbra** should be owner of the group):
   `ll /opt/zimbra/postfix/conf/infowatch`
   `chown zimbra:zimbra /opt/zimbra/postfix/conf/infowatch`
5. Convert transport file to DB:
   `postmap /opt/zimbra/postfix/conf/infowatch`
6. Add transport file before the default file:
   `zmlocalconfig -e postfix_transport_maps="hash:/opt/zimbra/postfix/conf/infowatch`
   `proxy:ldap:/opt/zimbra/conf/ldap-transport.cf"`
7. Make sure, that relay_domains parameter of **main.cf** file contains all domains processed by server:
   `mcedit /opt/zimbra/postfix/conf/main.cf`
   Find or create line:
   `relay_domains = mydomain.com, mydomain.org, dlp.iw`

#### Configuring BCC

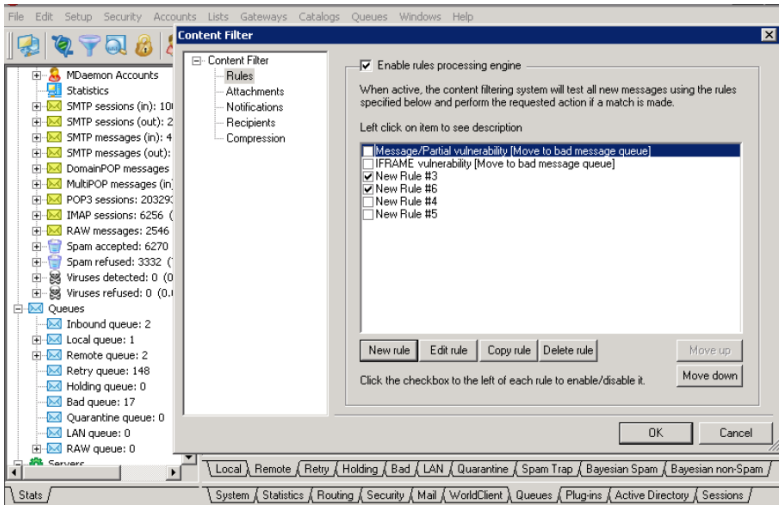
1. Add the following line to **/opt/zimbra/postfix/conf/main.cf** file:
   `/opt/zimbra/postfix/conf/main.cf`
2. Reboot Zimbra:
   `zmcontrol restart`

## Forwarding BCC with MDaemon

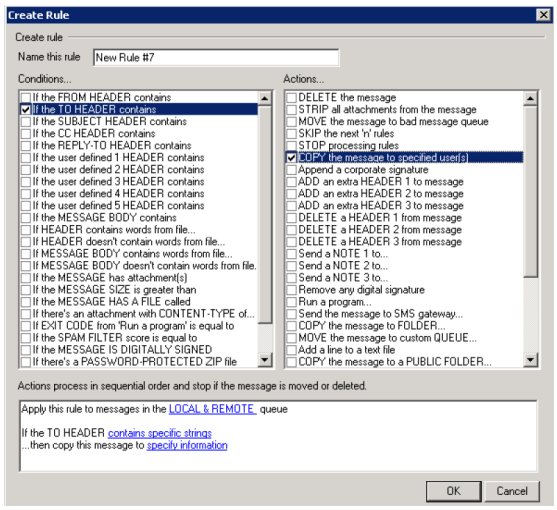
In MDaemon mail client there is **Content Filter** option, which can be used to configure incoming /outgoing mail filtering.

1. Open MDaemon and go to **Security > Content Filter** tab.

2. Go to **Rules** tab. Press **New rule** button:




3. In the left column choose action condition. In the right column choose corresponding action:




4. Use blue sections to add values to rules.
5. Click **Add** and **OK**.

## Configuring Postfix server in Traffic Monitor system

Necessity to configure built-in Postfix is being determined depending on System deployment scheme and whether TM server is installed on the same computer with database:

| **System deployment option** | | **Configuring Postfix** |
|---|---|---|
| SMTP traffic delivery is being performed by corporate mail server. Traffic Monitor system receives only a copy of SMTP traffic. It is recommended to configure Postfix for proper traffic reception | TM server is installed separately from database (kickstart key **IWTMX**) | Mandatory |
| | | Performed by default |

| System deployment option | | Configuring Postfix |
|---|---|---|
| | All components are installed on one server (kickstart key **IWALLX** or **IWTMSX**) | |
| Traffic Monitor system performs SMTP traffic interception and delivery through integration with Postfix | TM server is installed separately from database (kickstart key **IWTMX**) | Mandatory |
| | All components are installed on one server (kickstart key **IWALLX** or **IWTMSX**) | Performed by default |
| System receives SMTP traffic copy through Sniffer | | It is not required |
| SMTP traffic interception is not required (for example, Traffic Monitor will only be used as Sniffer) | | It is not required |

For proper interaction between InfoWatch Traffic Monitor and built-in Postfix mail server make the following changes to **/etc/postfix/main.cf** and **/etc/postfix/master.cf** configuration files:

1. Enter the system using **root**:
   `su - root`
2. In **main.cf** file set value for `inet_interfaces` parameter in accordance with recommendations on Postfix web page: http://www.postfix.org/postconf.5.html.

   > **Note:**
   >
   > In most cases it is sufficient to set value of parameter
   > `inet_interfaces = all`

3. In **main.cf** file set value for `message_size_limit` parameter in accordance with recommendations on Postfix web page: http://www.postfix.org/postconf.5.html.

   > **Note:**
   >
   > Default parameter value is
   > `message_size_limit = 50000000`

4. In case InfoWatch Traffic Monitor will participate in SMTP traffic delivery (see "Inline"):

- in **main.cf** file configure `relayhost` parameter. As a value enter the IP address of the corporate mail server to which SMTP letters will be transmitted after analysis in Traffic Monitor.
- edit **master.cf** file by writing the following lines to the end of file:

> **Warning!**
>
> A string specifying the service option must start with a space. For example: "`-o <option specification>`"

```
127.0.0.1:2020   inet  n   -   n  -   21   smtpd
     -o content_filter=
     -o local_recipient_maps=
     -o relay_recipient_maps=
     -o smtpd_restriction_classes=
     -o smtpd_client_restrictions=
     -o smtpd_helo_restrictions=
     -o smtpd_sender_restrictions=
     -o mynetworks=127.0.0.0/8
     -o strict_rfc821_envelopes=yes
     -o smtpd_error_sleep_time=0
     -o smtpd_soft_error_limit=1001
     -o smtpd_hard_error_limit=1000
     -o myhostname=<$hostname>
```

5. In **main.cf** file check, that mynetworks parameter has subnetwork specified, where mail servers will be located.
6. In **master.cf** file add the following line to provide transmission of mail to TM for check:
   `The n inet SMTP    -    n   -   -   smtpd  -o content_filter=smtp:127.0.0.1:2025`

> **Note:**
>
> Installing with the help of installation program (**kickstart**) this setting is being performed automatically.

7. Check the correctness of configuration files the syntax:
   `service postfix check`
8. Restart Postfix:
   `service postfix restart`

9. Check availability of Postfix port **25** using the following command in command line:
   `telnet <TM_ip> 25`
   where `<TM_ip>` - IP address of Traffic Monitor server where Postfix has been configured.
   As an output of this command the following message should appear:
   `Connected to mail.server.com`

> **Note:**
>
> In case Telnet client is not installed, you can install it as MS Windows 2008-2012 component or use Putty application instead.

In case it was not possible to establish connection, perform a step by step check of subnets and ports settings depending on System configuration.

### 2.4.2 Configuring POP3 Traffic Interception

1. Configure server (servers) for working with SPAN, or Port Mirroring (see "Configuring Server to work with SPAN, or Port Mirroring Technology").
2. Make sure, that `Hi Port` parameter of `capstack` section in **/opt/iw/tm5/etc/sniffer.conf** configuration file has value `110`:

```
"ListenAreas": {
"capstack": {
"Balancer": "IpPref",
"Interface": "eth1",
"MaxClient": 16,
"QueueMemorySizeInBytes": 67108864,
"Rules": [
{
"HiPort": 110,
"IP": "0.0.0.0",
"LoPort": 110,
"Mask": "0.0.0.0",
"Policy": "ACCEPT"
```

3. Specify value `true` for `pop3` parameter of **/opt/iw/tm5/etc/capstack.conf** configuration file.

### 2.4.3 Configuring HTTP Traffic Interception

For this traffic interception method, see "HTTP Traffic Interception Scheme".

### SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see "SPAN, or Port Mirroring").

2. Make sure, that SMTP traffic interceptor autorun is enabled in **proxy.conf** configuration file, located in /ort/iw/tm5/etc directory, in section Startup:
```
"Startup": {
"Enabled": true,
"http": true
```
3. Make sure, that autostart of all processes, which participate in traffic interception and analysis, is enabled:
**iw_sniffer, iw_proxy_HTTP, iw_warpd, iw_cas, iw_loader** (see "Enabling and disabling autorun processes").

## Inline Mode

> **Note:**
>
> In this item, «inline» mode of interception is described, which is being transmitted by ICAP protocol – do not confuse with «inline» mode for SMTP traffic.

**To configure inline transfer mode, issue the following actions:**

1. Learn this working schema (see "Intercepting traffic, transmitted via ICAP protocol").
2. Configure HTTP requests interception parameters on proxy server (see "Configuring ICAP").

## 2.4.4 Configuring HTTPS Traffic Interception

For this traffic interception method, see in "HTTPS Traffic".

## Inline Mode

> **Note:**
>
> In this item, «inline» mode of interception is described, which is being transmitted by ICAP protocol – do not confuse with «inline» mode for SMTP traffic.

**To configure inline transfer mode, issue the following actions:**

1. Learn this working schema (see "Intercepting traffic, transmitted via ICAP protocol").
2. Configure HTTP requests interception parameters on proxy server (see "Configuring ICAP").
3. Enable HTTPS traffic parsing on proxy-server.

> **Note:**
>
> This setting depends on proxy-server modification. You can get actual information on configuring proxy-server from its manual.

4. Add certificate to the list of trusted root browser certificates of each Workstation, where outgoing HTTPS traffic is supposed to be controlled.

> **Note:**
>
> Get configuration information from browser documentation.

### 2.4.5 Configuring SMTP Traffic Interception

For this traffic interception method see "ICQ Traffic Interception Scheme".

### SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see "SPAN, or Port Mirroring").
2. Make sure, that SMTP traffic interceptor autorun is enabled in **proxy.conf** configuration file, located in `/ort/iw/tm5/etc` directory, in section `Startup`:

```
"Startup": {
"Enabled": true,
 "icq": true
```

### 2.4.6 Configuring NRPC Traffic Interception

### SPAN, or Port Mirroring

1. Configure server (servers) to work with SPAN technology, or Port Mirroring (see "SPAN, or Port Mirroring").
2. Open capstack.conf configuration file, which is located in `/ort/iw/tm5/etc` directory.
3. Make sure, Usedprocessors section has NRPC traffic interceptor enabled:

```
"UsedProcessors": {
"nrpc": true,
```

4. Make sure, Processors section has NRPC traffic transmission enabled:

```
"processors": {
"nrpc": {
"TrackExternal": true,
"TrackInternal": true
 },
```

5. Make sure, `Startup` section has autostart enabled:

```
"Startup": {
"Enabled": true
  },
```

6. Save changes in the **capstack.conf** file.
7. Restart **capstack** process:
   `service iwtm restart capstack`

## 2.4.7 Receiving Objects Intercepted by InfoWatch Device Monitor

1. Install and configure Traffic Monitor Server part (see document "InfoWatch Traffic Monitor. Installation guide", article "Installing Traffic Monitor Server (TME Node Server)").
2. Setup event transmission from Device Monitor to Traffic Monitor server (see document «InfoWatch Device Monitor. User guide», article "Integration with Traffic Monitor Versions").
3. Setup object analysis parameters (see document «InfoWatch Traffic Monitor. User guide», article "Technologies Section").

## 2.4.8 Revision of Files from the Corporate Network

For this traffic interception method see "Revision of Files from the Corporate Network".

File server contents and network resources analysis is only possible after installing special module under MS Windows Server OS.

1. Install and configure Traffic Monitor Server (see document "InfoWatch Traffic Monitor. Installation guide", article "Installing Traffic Monitor Server (TME Node Server)").
2. Install and configure Crawler (see document "InfoWatch Traffic Monitor. Installation guide", article "Installing the Crawler Subsystem").
3. Configure main Crawler scanner parameters (see document "InfoWatch Traffic Monitor. Administration guide", article "Configuring Crawler Interceptor").
4. Configure object analysis parameters (see document "InfoWatch Traffic Monitor. Administration guide").

## 2.4.9 Configuring IMAP4 Traffic Interception

1. Configure server (servers) for working with SPAN, or Port Mirroring (see "SPAN, or Port Mirroring").
2. Make sure, that `Hi Port` parameter of `capstack` section in **/opt/iw/tm5/etc/sniffer.conf** configuration file has value `143`:

```
"ListenAreas": {
"capstack": {
"Balancer": "IpPref",
"Interface": "eth1",
"MaxClient": 16,
"QueueMemorySizeInBytes": 67108864,
"Rules": [
{
```

```
"HiPort": 143,
"IP": "0.0.0.0",
"LoPort": 110,
"Mask": "0.0.0.0",
"Policy": "ACCEPT"
```

3. Specify value `true` for imap4 parameter of **/opt/iw/tm5/etc/capstack.conf** configuration file.

# 2.5 Process autorun

This section contains fratures of System's processes autostart:

- Checking process autorun;
- Enabling and disabling autorun processes.

General information on working with processes is available in chapter "Traffic Monitor Server Processes".

## 2.5.1 Check of process autostart

> **Warning!**
>
> Disable autostart of unlicensed processes responsible for traffic interception. This allows you to reduce the number of messages in the log.

When you divide servers into the main server, interception server and web console server, make sure, that autostart is configured according to notes in the table.

Autostart must be enabled only for processes, which this copy of Traffic Monitor server needs for proper operation:

| Process | By default autostart is enabled |
|---|---|
| iw_adlibitum | Yes<br>**Note:** Process must operate only on the main server |
| iw_agent | Yes |
| iw_kicker | Yes<br>Process combines the following services:<br>• `selection`<br>• `blackboad`<br>• `systemcheck`<br>• `agent` |

| Process | By default autostart is enabled |
| --- | --- |
| | • `xapisamplecompiler`<br>• `export`<br>• `samplecompiler`<br>• `report`<br>• `import`<br>• `notifier`<br>• `crawler`<br>To enable service, set `1` value in `kikers` section **web.conf** configuration file.<br>To enable service, set `0` value in `kikers` section **web.conf** configuration file.<br>**Note:** Process must operate only on the server with web console |
| iw_blackboard | Yes |
| iw_bookworm | Yes |
| iw_capstack | Yes |
| iw_cas | Yes |
| iw_configerator | Yes<br>**Note:** Process must operate only on the server with web console |
| iw_deliver | Yes |
| iw_expressd | Yes |
| iw_icap | Yes |
| iw_indexer | Yes<br>**Note:** Process must operate only on the main server |
| iw_licensed | Yes<br>**Note:** Process must operate only on the main server |
| iw_loader | Yes |

| Process | By default autostart is enabled |
|---|---|
| iw_luaengined | Yes |
| iw_messed | Yes |
| iw_proxy_http<br>iw_proxy_icq<br>iw_proxy_smtp | Yes |
| iw_qmover_client | No |
| iw_qmover_server | No |
| iw_sample_compiler | Yes |
| iw_serman | Yes |
| iw_smtpd | Yes |
| iw_sniffer | Yes |
| iw_system_check | Yes |
| iw_updater | Yes |
| iw_warpd | Yes |
| iw_whiteboard | Yes |
| iw_xml2liro | Yes |

### A note:

To delete **iw_kicker** process from the server, delete **iwtm-webgui** package:

```
rpm -e iwtm-webgui
```

For more information on how to enable autostart for processes, see "Enabling and disabling autostart of processes".

## 2.5.2 Enabling and disabling autorun processes

**To enable/disable process autorun (example for iw_sniffer service):**

1. For correct setting modification stop Traffic Monitor server processes Traffic Monitor:
   `service iwtm stop`
2. In **/opt/iw/tm5/etc/sniffer.conf** file complete the settings:
   To enable the autorun of a process, in the process section set:
   `"Startup" : {"Enabled" : true}`
   To disable the autorun of a process, in the process section set:
   `"Startup" : {"Enabled" : false}`

   **Warning!**

   The enabling and disabling of iw_proxy service's modules is performed in the following way:

   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}`
     – enabling all modules;
   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}`
     – enabling iw_proxy_http module;
   - `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}`
     – disabling all modules.
3. Start Traffic Monitor Server processes:
   `service iwtm start`

# 2.6 Configuring OCR extractors

Configuring OCR for different interceptors OCR is performed in the following configuration files:

- **expressd.conf** - you should specify value `true` for each interceptor for which the OCR usage should be enabled (see "The Expressd Section, Ocr Parameter")
- **messed.conf** - you should specify value `true` for `OCR` parameter if you need to enable the `OCR` usage for letter transferred through mail relay-server (see "The messed.conf Configuration File ").
- **warpd.conf** – In section `Warp` specify value for `EnableOCR` parameter `true`.
- **proxy.conf** – In section Http or Icq it is required to change `OCR` parameter value to `true` (see " The proxy.conf configuration file")
- **analysis.conf** – In section `Analysis` it is required to change `OCR` parameter value to `true`

The recognition of a text from extracted images is performed by one of OCR extractors: either Tesseract 3.0 or ABBYY FineReader Engine 11.

When installing with the help of installation program (**kickstart**) to server part of the System both OCR-extractors are installed. Tesseract 3.0. is set to work by default.

Functional limitations of extractors are given in the table below:

| Functionality | Tesseract 3.0 | ABBYY FineReader Engine 11 |
|---|---|---|
| Recognition of the image rotation angles | - | 0(+/-20) , 90(+/-20), 180(+/-20) and 270(+/-20) degrees |
| Recognition of color images | - | + |
| Image correction | - | + |
| Recommended image resoltion | 300dpi for text with a font size from 10pt<br>400-600dpi for text with a font size of 9pt and less | 300dpi for text with a font size from 10pt<br>400-600dpi for text with a font size of 9pt and less |

**To set ABBYY FineReader Engine 11 to work:**

1. Delete **/opt/iw/tm5/bin/iw_image2text** symlink.
2. Create symlink:
   `ln -s /opt/iw/tm5/bin/iw_image2text_fre /opt/iw/tm5/bin/iw_image2text`

**To replace ABBYY FineReader Engine 11 with Tesseract 3.0:**

1. Delete **/opt/iw/tm5/bin/iw_image2text** symlink.
2. Create symlink:
   `ln -s /opt/iw/tm5/bin/iw_image2text_ts /opt/iw/tm5/bin/iw_image2text`

# 2.7 Configuring Email Notifications for Users and Employees

Management Console user has the ability to setup email notifications for user or employee. Alerts are sent if the certain rules in the policies were operated (see document "InfoWatch Traffic Monitor. User Guide"). You should:

- define email address from which notifications will be sent to users or employees;
- adjust mail delivery via Postfix.

**To configure e-mail address to send notifications:**

1. Connect to the database as the owner of the schema.
2. Set necessary email address of the sender as a value of `NOTIFY_SENDER` attribute in the *SETTING*, table.

**To check if letters are sent via Postfix:**

Execute:

```
sendmail -v <employee@company.com> < <sample.log>
```

where:

- `<employee@company.com>` - email address of the notification recipient;
- `<sample.log>` - text file containing the body of the letter (it is recommended to use simple text file less than 1MB for the check).

Adjust mail delivery via Postfix if letters are not sent.

**To adjust mail delivery via Postfix:**

1. Open **/etc/postfix/main.cf** file
2. Set required mail server for `relayhost` attribute:
   ```
   relayhost = <mail.company.ru>
   where <mail.company.ru> - required mail server
   ```

   > **Note:**
   >
   > If **/etc/postfix/main.cf** file does not have a line containing relayhost attribute, add the necessary line.

3. Reboot Postfix with help of the following command:
   ```
   service postfix restart
   ```
4. Check the mail delivery with help of the following command:
   ```
   sendmail -v <employee@company.com> < <sample.log>
   ```
   where:

- `<employee@company.com>` - email address of the notification recipient;
- `<sample.log>` - text file containing the body of the letter (it is recommended to use simple text file less than 1MB for the check).

# 2.8 Limiting the number of events that can be found

You can specify a limitation for the maximum number of events that will be displayed in the Management Console as a result of applying filter. For this, in the *SETTING* table of a database, specify a desired value for the *query_stop_count* attribute. The default value is 10.000.

# 2.9 Configuring InfoWatch Device Monitor Server

Server is configured with `InfoWatch.DeviceMonitor.Server.exe.config` XML configuration file. Configuration file is stored in the same directory as Server executable file `InfoWatch.DeviceMonitor.Server.exe`.

By default, after its installation the Server is located in

`C:\Program Files\InfoWatch\Device Monitor\Server`.

You can view and edit configuration file with any text or XML Editor. UTF-8 File Encoding.

`<configuration>` is the root element of configuration file. Root element includes child elements (configuration sections). The following table contains configuration file structure and its partitions description. Section links provide detailed information on their configuration.

> **Important!**
>
> It is extremely not recommended to edit the configuration file without InfoWatch engineer assistance.
>
> When editing of file is finished, please restart Device Monitor Server.

| Configuration section | Description |
|---|---|
| <configSections> | Service section. Describes all remaining sections.<br>You should not edit this section. |
| <runtime> | Contains Microsoft .NET framework environment settings. These settings are required for correct Server operation.<br>In `<runtime>` section the `gcServer` element is specified for garbage collector configuration. Element features `enabled` attribute with `true` (parallel garbage collection is enabled) or `false` value (parallel garbage collection is disabled).<br>It is not recommended to edit this section. |
| <applicationSettings> | Contains individual Server modules settings, such as ports, buffer size, time-out, etc. |
| <system diagnostics> | Contains logging settings. Logging can be useful for Server components diagnostics. |

If you need to delete temporary files generated by Device Monitor, you can do it by the special utility: see details in "Deleting Device Monitor Temporary Files".

## 2.9.1 <applicationSettings> Section

You can use `<applicationSettings>` section to configure individual Server modules. There are six modules. All sections have the same structure: Each section includes a set of elements for module configuration. Each `<setting>` element has the following attributes:

- `name` - setting name.

- `serializeAs` - data serialization method. Data is always serialized as a string (string data type).

Module parameters are defined by <value> child element. For example:

```
<setting name="RemotingPort" serializeAs="String">
   <value>15003</value>
</setting>
```

Each module parameters are described in the following table.

| Section of configuration file | Description |
|---|---|
| `<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings>`<br>Server kernel configuration | |
| `RemotingPort` | TCP port processing Management Console service connections.<br>Default value `15003` (it is not recommended to change this value) |
| `CultureName` | Language of module diagnostic and other messages.<br>Possible values:<br>• `ru-RU`<br>• `en-US` |
| `MachineName` | IP address of network interface used by the Server to accept Management Console connections.<br>Default value `127.0.0.1`. Youcanonlychangethisvalue, if the Server has 2 or more network interfaces. In this case, you must explicitly specify interface address used by the Server to accept incoming connections from different instances of Management Console |
| `CheckServerSettingsInterval` | With clustering enabled - database synchronization period (in seconds). After this, the Server sends a request to security schema in order to retrieve changes implemented by the main Server that uses the same database.<br>Default value is `10` |
| `<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings>`<br>Settings of the module interacting with the database | |
| `DatabaseType` | Database types.<br>Possible values:<br>• `Oracle`<br>• `Microsoft`<br>• `PostgreSql` |
| `ConnectionString` | Database connection string. It must comply with ADO.NET connection string rules.<br>For example:<br>`Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security=True` |

| Section of configuration file | Description |
|---|---|
| `CultureName` | Language of module diagnostic messages and other messages.<br>Possible values:<br>• `ru-RU`<br>• `en-US` |
| `ConnectionPoolSize` | Number of DB connections to open and use by the server.<br>The default value is `20`.<br>**Note**: The value must exceed the value of the `NumberOfConnections` parameter. |
| `CommunicationPort` | Port number used for server connection with Deploy agent when installing a Client through task engine. It is not recommended to change this value when operating.<br>Default value is `15505`. |
| `UpdateStatusTimeOut` | Time interval of updating the job execution state at remote computer. With this interval server survey remote computers where the Client is deployed about installation state to display on the Management Console.<br>Default value is `60`. |
| `<InfoWatch DeviceMonitor.Server.Gui.Properties.Settings.>`<br>Management Console interface module configuration | |
| `CultureName` | Language of module diagnostic messages and other messages.<br>Possible values:<br>• `ru-RU`<br>• `en-US` |
| `InitialLeaseTime` | Management Console valid connection time (in minutes) |
| `RenewOnCallTime` | Time (in minutes) to prolongate Console-Server connection lifetime |
| `<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings>`<br>Client connections module configuration (managed workstations) | |
| `Backlog` | Pending client connections queue. Default value 128 |
| `CultureName` | Language of module diagnostic messages and other messages.<br>Possible values:<br>• `ru-RU`<br>• `en-US` |

| | |
|---|---|
| `ShadowCopyTempDir` | Full path to temporary shadow copies pending submission to InfoWatch Traffic Monitor.<br>Default value:<br>`C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir` |
| `DmpV1Adress` | List of IP addresses (with enumeration separator "; ") used by server for listening to ports. The following values are possible:<br>• `AllAny` – all ports of IP addresses available for the computer (default value);<br>• `AllIp4` – ports of all version 4 IP addresses;<br>• `AllIp6` – ports of all version 6 IP addresses. |
| `Dmpv1TraceLevel` | Client-Server protocol trace level.<br>Possible values:<br>• turn tracing off (default value);<br>• only trace packet information;<br>• completetracing.<br>**Note:** The tracing will be output to the listener of diagnostic messages (the Windows Log file by default) only of the setting value is 3 and log level fir the module filter is `Verbose` (see "<system.diagnostics> Section"). |
| `Dmpv1TraceClients` | List of Client IP addresses (with enumeration separator "; ") that require tracing.<br>`All` means that tracing is carried out for all Clients. |
| `Dmpv1ConnectionsLimit` | Number of simultaneously processed TCP/IP connections with Clients.<br>Default value is `200`. |
| `Dmpv1ConnectionsQueueLimit` | Max number of connections awaiting for processing. If the number excesses, connections are reduced to `Dmpv1ConnectionsQueueLengthAfterCut` parameter value.<br>Default value is `500`. |
| `Dmpv1ConnectionsQueueLengthAfterCut` | Number of connections after queue reduced because of max size excesses.<br>Default value is `250`. |
| `TimeoutPeriodSeconds` | Timeout to close hanged Client-Server connection: partially created shadow copies will be deleted, sending of shadow copies will be repeated in next established connection.<br>Default value is `120`. |
| `SSLPort` | Port number for encrypted connections.<br>Default value is `15004`. |

| Section of configuration file | Description |
|---|---|
| `<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings>`<br>Traffic Monitor Server connector basic configuration | |
| `DBPollTime` | Database query period (in milliseconds) checking for database events |
| `CultureName` | Language of module diagnostic messages and other messages.<br>Possible values:<br>• `ru-RU`<br>• `en-US` |
| `NumberOfConnections` | Number of InfoWatch Traffic Monitor connections.<br>The default value 4. Maximum value is `32`.**Note**: The value must not exceed the value of the `ConnectionPoolSize` parameter. |
| `QueueSendLimit` | Maximum number of events transferred from database to InfoWatch Traffic Monitor in a single transaction.<br>Default value is `200`. |
| `ShadowCopyTrasferBlockSize` | Size of shadowcopy data block sent to Traffic Monitor server, in MB.<br>Default value is `16`. |
| `<InfoWatch DeviceMonitor Database.Core.Properties.Settings>`<br>Low-level database driver configuration | |
| `CultureName` | Language of module diagnostic messages and other messages.<br>Possible values:<br>• `ru-RU`<br>• `en-US` |
| `MaxConnectionWaitingTime` | Timeout for free connection from the pull, seconds. Default value `300`. |
| `CommandTimeoutSeconds` | Runtime of the operation or queue, sec. Default value is `30`.<br>**Note:** this setting is not applied for Oracle DBMS. |
| `LongCommandTimeoutSeconds` | Runtime of the long operation or queue, seconds. Applied when runtime is a vast interval. Default value is `0` (endless).<br>**Note:** this setting is not applied for Oracle DBMS. |

### 2.9.2 <system.diagnostics> Section

Server diagnostics section. It includes the following elements:

- `<trace>`. Diagnostics module general settings.
- `<sources>`. Individual Server components diagnostics settings.
- `<switches>`. Managing diagnostic system's overall level of detail. Includes detalizer definitions. Typically, there is a single detilizer. If different modules require different detalisation settings, you should use a filter. General detalizer's value must contain maximum detail.

***<trace>* element**

Used to describe global module diagnostics settings. In this element you can specify message margins and diagnostics data saving parameters.

***<sources>* element**

Used to configure individual application modules. Includes <source> child elements - one for each application module (see Server module list in "<applicationSettings> section").

The list of modules also includes secondary ones which are needed for debugging output for main components:

- `InfoWatch.DeviceMonitor.Server.FileIdentification.Core` - module describing the signatures object model;
- `InfoWatch.DeploymentSubSystem` - module of the subsystem responsible for deployment on computers;
- `InfoWatch.DeviceMonitor.EventPostProcessorManager` - module for post-processing of print events;
- `InfoWatch.DeviceMonitor.ScreenShotStorage` - module for saving screenshots on the file system;
- `InfoWatch.DeviceMonitor.Server.Remote.Install` - module for launching the remote installation\update\uninstallation of the Agent on the computer.

`<source>` element has the following attributes:

- `name`. Server module name.
- `switchName`. Name of the module that defines diagnostics (detalizer's) level of detail.
- `switchType`. Type of the module that defines diagnosis level of detail. Is always set to `System.Diagnostics.SourceSwitch`.

Each `<source>` element also contains a definition for diagnostic messages receiver (`<listeners>`). Diagnostic messages can be received by:

- Windows application log (Application log);
- system debug output (can be viewed with special tools like DebugView);
- text file.

`<source>` element has child element `<listeners>`. This element contains parameters of diagnostic messages receiver. `<listeners>` element may contain the following child elements:

- <add>. Add a new diagnostic messages receiver
- <remove>. Deleting diagnostic messages receiver. You can only apply it to remove default message receiver (Windows application log). To this end, set element name to `Default`: `<remove name="Default" />`

### *<add>* element

This item adds diagnostic messages receiver to Server module. Element contains the following attributes:

- `name`. Diagnostic messages receiver name.
- `type`. Diagnostic messages receiver type.
- `initializeData`. Server module ID. Typically, this value is the same as Server module name. If Windows application log is the receiver, this information appears in the source column.

Receiver type is fully qualified receiver name from .NET framework library or proprietary type that implements the required diagnostic messages receiver interface.

.NET framework library contains the following diagnostic messages receiver types:

- `System.Diagnostics.EventLogTraceListener`. Windows application log
- `System.Diagnostics.ConsoleTraceListener`. Console application message output
- `System.Diagnostics.TextWriterTraceListener`. Text file output
- `System.Diagnostics.DefaultTraceListener`. Debug Windows output (enabled by default).

<add> element also contains diagnostic messages filter. This filter only displays the messages with level of detail exceeding the filter parameters. It features the following levels of detail (listed in descending priority order):

- `Verbose`. Debug level. All events are logged. This level can only be used for System debugging. This level does not allowed for a system running in normal mode, since it cuts the performance significantly.
- `Information`. Information level. Registers the events that are not related to errors, for example, information on server changes.
- `Warning`. Warning level. Registers non-critical System errors, such as an unexpected disconnection from the Server, connection timeout, etc.
- `Error`. Error level. Records errors that cause System malfunction (i.e., errors that require troubleshooting).
- `Critical`. Critical level. Registers serious malfunctions that can lead to System shutdown.

### Example 1

Detalizer features *Verbose* logging level, while module filters feature *Warning* level. Then detalizer ignores *Warning*, *Error* and *Critical* events, but filters out *Information* and *Verbose* events.

### Example 2

Detalizer features *Error* logging level, while module filters feature *Warning* level. In this case, detalizer ignores *Error* and *Critical* events, but filters out *Warning*, *Information* and *Verbose* events. This happens because overall System level of detail is *Error*, i.e. only *Error* events and higher are registered regardless the filter settings.

***<remove>* element**

Deleting message receiver. It is usually used to remove default receiver that displays diagnostic messages in Windows debug output:

```
<remove name="Default" />
```

***<switches>* element**

Defines Server detalizers. Typically, there is only one detalizer, which sets the global (for entire Server) level of detail the diagnostic system. If individual Server modules require lower level of detail, you can use filters.

`<switches>` element contains only one child element by default:

```
<add name="eventLog" value="Warning"/>
```

Level of detail is specified as `value` attribute.

## 2.9.3 Deleting Temporary Device Monitor Files

InfoWatch Device Monitor provides a means for deleting the files generated by the System, namely:

- all files from the temporary files directory of the operating system (%Temp%);
- data from file queue of Device Monitor events processing (`C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir` by default; see information on the path configuring in "<applicationSettings> Section").

The deleting is performed by `RemShadowCopyFiles` utility located in the Server installation folder (`C:\Program Files\InfoWatch\DeviceMonitor\Server` by default).

The launching of the utility should be performed by administrator account having rights for reading and writing in directories containing deleting files.

> **Important!**
>
> The System will stop the proceeding of incoming events for a time when deleting procedure runs.
>
> The procedure will delete all the data on events which were not proceeded by the moment of deleting start.

**To delete temporary files:**

1. Log on at the InfoWatch Device Monitor Server where you need to delete temporary files.
2. Run `RemShadowCopyFiles` utility.
3. Confirm deletion by pressing **Y**.

The utility will stop all Device Monitor services, delete temporary files and start Device Monitor services again.

> **Important!**
>
> When deleting temporary files from %Temp% system folder the access denial can arise: there can be some files created and used by another processes irrelevant to the System.

# Working in Web-Console

A set of System management actions can be performed by Administrator in a simplified way, via the Management console, which is available from the browser of any Workstation in the local network.

Major steps of Administrator to manage the System via the Management console are described in the following items:

- Logging on and off the Web-Console Interface;
- Managing LDAP Catalogues Integration;
- Managing System Users and their Roles;
- Managing Licenses;
- Healthcheck;
- Managing Services;
- Collecting the Diagnostic Data;
- User Actions Audit;
- Integrity Monitoring;
- Plugins.

## 3.1 Logging on and off the Web-Console Interface

**To log into a web-console:**

1. Open Google Chrome internet-browser (in case you do not have browser installed, download it here: http://www.google.com/intl/ru/chrome/browser/).
2. In the address line, type in InfoWatch Traffic Monitor address.
3. In **Login** field, specify user name.
4. In **Password** filed, specify password.
5. Press **Enter**.

> **Warning!**

To ensure data safety it is strictly recommended to leave web-console upon all works completion. To do this, select **Logout** from the upper right menu.

System is configured to perform automatic exit after 30 minutes timeout.

# 3.2 Managing LDAP Catalogues Integration

Configuring the synchronization with LDAP catalogues is performed in **Administration -> LDAP Synchronization** section.

**Warning!**

If you have Adblock Plus installed for the browser then you should disable this extension to provide a correct operation of this web-console section.

In the left part of working area **of LDAP server** is located toolbar
List of servers, LDAP synchronization with which has been set, is being displayed under the toolbar.
The toolbar contains a set of tools for working with connections.
In the central part of the working area chosen connection parameters are displayed:

| Parameter | Description |
|---|---|
| Server name | Connection identifier used in the management console |
| Server type | Indicates whether is used *Active Directory* or *Domino Directory* |
| Active | Indicates if the synchronization is performed according to specified timetable |
| Synchronization period | Type of synchronization repeating |
| Retry parameters | Value of synchronization repeating period<br>***For example***, with specified values<br>• *Synchronization period* – `Every N minutes`;<br>• *Retry parameters* – 60 `minutes`,<br>synchronization will be performed every 60 minutes. |
| LDAP server | Network identifier of the server with which LDAP catalogues the synchronization is performed |
| Global LDAP port | Port for global LDAP catalogue connection.<br>**Note:** This parameter is only available for Active Directory |
| LDAP port | Port for domain catalogue connection |

| Parameter | Description |
| --- | --- |
| Use global catalogue | Indicates if the global LDAP catalogue is used for synchronization<br>**Note:** This parameter is only available for Active Directory<br>**Warning!**<br>Synchronizing with Windows 2008 R2 or Windows 2012 catalogue, set parameter value as `Don't use`. |
| LDAP request | Domain (LDAP base), in which AD data search is being performed.<br>**Note:** This setting is not required for the Domino Directory<br>To improve AD search you can use separate hierarchy levels of the base.<br>***For example***, to use as a base branch `Users`, located in company domain, it is necessary to assign to parameter **Filtration attributes** the following value:<br>`cn=users,dc=company,dc=com` |
| Login | Login for accessing the synchronization server |
| Password | Password for accessing the synchronization server |
| Last synchronization time | Data and time of ending the last synchronization |
| Last synchronization status | Result of the latest synchronization |
| Next synchronization | Data and time of next synchronization |

Configuring LDAP catalogues integration is described below:

- Creating connection to server;
- Editing connection to server;
- Deleting connection to server;
- Start synchronization with server manually..

## 3.2.1 Creating connection to server

**To create connection to server:**

1. Go to **Administration -> LDAP Synchronization**.
2. On the toolbar click  **Create**.
3. Specify parameters for new connection (see "Managing LDAP catalogues integration").
4. Click **Check connection**, to perform control check of connection to server.

5. Click **Save**.

### 3.2.2 Editing connection to server

**To edit connection to server:**

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Edit**.
4. Change connection parameters (see "Managing LDAP catalogues integration").
5. Click **Check connection**, to perform control check of connection to server.
6. Click **Save**.

### 3.2.3 Deleting connection to server

**To delete existing Server connection:**

1. Go to **Administration -> LDAP Synchronization**.
2. By left-click select required server.
3. On the toolbar click  **Delete**.

> **Note:**
>
> To delete several connections at a time, highlight them (for example, holding **<SHIFT>** or **<CTRL>** ) and click **Delete** .

4. In the opened window click **Yes**.

### 3.2.4 Running Synchronization with Server Manually

**To run synchronization with Server manually:**

1. Go to **Administration -> LDAP synchronization**.
2. Left-click at the target server on the left.
3. Click  **Starting synchronization** button located on the toolbar.

Information on the synchronization results will be displayed in *Last synchronization, Status of the synchronization, Next synchronization status* strings.

> **Note:**

If the *Synchronize* connection attribute has Every N minutes or Every N hours value then the automatically synchronization will be performed with specified frequency after last manual running.

**Warning!**

Synchronization will be performed according to Traffic Monitor server time. If management console is located in different time zone, then specifying synchronization time is required to be done considering difference between time zones of server and management console.

# 3.3 Managing System Users and their Roles

To manage System users the following entities are used:

- *User* – user's account (see "Users");
- *Role* – a set of rights which can be assigned to User (see "Roles");
- *Visibility scope* – a set of attributes of interception objects: the objects with those attributes will be available to specified users only (see "Visibility Scopes").

## 3.3.1 Users

Configuring the System users list is performed in the **Administration -> Users and Roles** section, the **Users** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of users displayed at the page) are located.

Account attributes are listed in the following table:

| Parameter | Description |
|---|---|
| *Login* | Name of user account |
| *Full name* | User's first name and second name |
| *Email* | User's e-mail address |
| Roles | List of roles assigned to the user |
| *Scopes* | List of visibility scopes available for the user |
| *Description* | Note to the account |

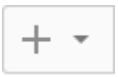
| Parameter | Description |
|---|---|
| Status | Indicates whether user role is active or passive |

You can perform the following actions while managing users:

- Creating User Account;
- Editing User Account;
- Deleting User Account;
- Changing User Account Password;
- Changing User Account State;
- Importing User Account from Active Directory;
- Assigning Role to a User;
- Creating Visibility Scope to User.

## Creating User Account

**To create user account:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar click  **Create User**.
4. In the opened window specify account parameters.

| Parameter | Description |
|---|---|
| *Login* | User account name |
| *Status* | Indicates if the user account is active or passive |
| *Interface language* | Language, which will be assigned to the interface of selected user account |
| *Password* | User account password<br>**Note:** See recommendations on password creation in Appendix A "User Name and Password recommendations". |
| *Confirm password* | User account password |
| *Email* | User email address |
| *Full name* | Full name of the user |

| Parameter | Description |
| --- | --- |
| *Description* | User account notes |

5. Click **Save**.

## Editing User Account

**To change existing user account parameters:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click  **Edit user** on a toolbar.
5. In the opened window change account attributes (see "Users").
6. Click **Save**.

## Deleting User Account

**To delete user account:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  **Delete user**.

> **Note:**
>
> To delete several accounts in one action, select them from the list (for example, by pressing **<SHIFT>** or **<CTRL>** ) and click **Delete user** .

5. In the opened window click **Yes**.

## Changing User Account Password

**To change user account password:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.

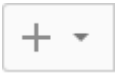
4. On the toolbar click  **Change password**.
5. In the opened window enter a new password to **Password** and **Confirm password** fields.

> **Note:**
>
> Recommendations for usernames and user passwords see in Appendix A "User Name and Password recommendations".

6. Click **Save**.

## Changing User Account State

**To change account state:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  and choose **Activate user** or **Deactivate user**.

> **Note:**
>
> You can change a status of any account except of **Administrator**.

## Importing User Account from Active Directory

You can easily create users by importing their accounts from Active Directory or Domino Directory.

> **Important!**
>
> If AdBlock extension is used in your browser, then disable this extension before importing user accounts, as AdBlock blocks the import.

**To import user account:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. On the toolbar click  **Import users from LDAP**.
4. In the opened window, specify LDAP server which stores the required account.

> **Note:**
>
> You can enter a part of login name to the **Search** field and click **Search**.

5. Flag required user accounts.
6. Click **Save**.

## Assigning Role to a User

**To assign role to a user:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Users** tab.
3. In the users list left-click at the target account.
4. Click  on the toolbar.
5. Choose **Set role** in the list (see "Roles").
6. Click **Save**.

## Creating Visibility Scope to User

**To create visibility scope to user:**

1. Go to the **Administration -> Users and roles** section.
2. Go to **Users** tab.
3. In the users list left-click at the target account.
4. On the toolbar click  .
5. Choose from Set visibility scope the list (see "Visibility Scopes").
6. Click **Save**.

## 3.3.2 Roles

To control redundant access to system settings, policies of different structural departments, interception objects and other important information, there is role system of access rights differentiation in InfoWatch Traffic Monitor.

Role is a set of rights which can be assigned to user. Assigning a role to user is described in " Assigning Role to a User".

Initially there are two predefined roles and the two preset user – roles **Administrator** and **Security officer** , which are accordingly assigned to Administrator and Officer users.

**Administrator** role provides an opportunity to carry out the initial configuration of the system (Managing users, roles, visibility scopes, licenses and LDAP sunchronization).

**Security officer** role has all rights except for initial setup.

Configuring the roles list is performed in **Administration -> Users and Roles** section, **Roles** tab.

In the work area the list of System users, toolbar and a drop-down menu (defining a number of roles displayed at the page) are located.

Role attributes are listed in the following table:

| Attribute | Description |
|---|---|
| *Name* | Role name |
| *Users* | First name and second name of the user |
| *Description* | Comment to a role |

You can perform the following actions while managing roles:

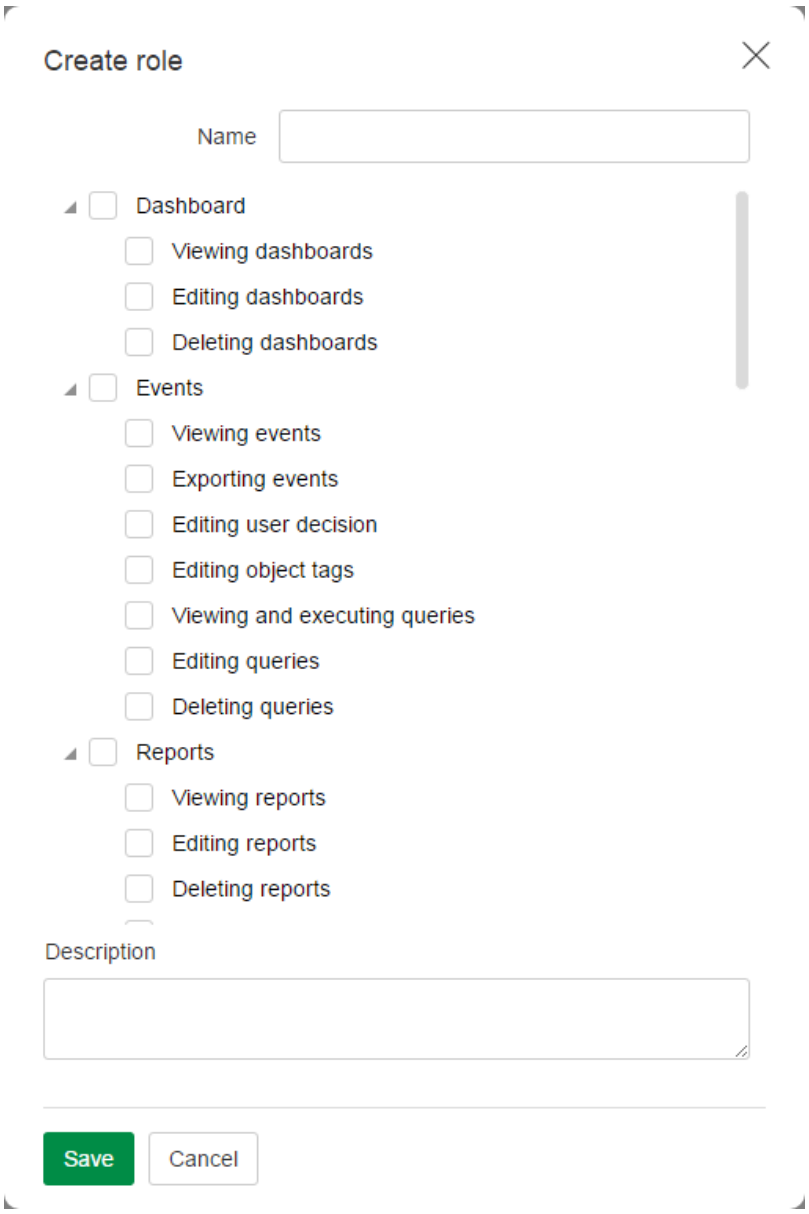
- *Creating a Role*;
- *Editing a Role*;
- *Deleting a Role*.

## Creating a Role

**To create a new role, follow the steps below:**

1. Go to section the **Administration -> Users and roles**.
2. Go to the **Roles** tab.
3. On the toolbar click  **Create role**.
4. In the opened window specify role attributes. Flag the privileges you want to assign to the role.

> **Note:**
>
> To expand / collapse privileges list, click ▶ or ◢ respectively.




**Picture 4. Creating a Role**

5. Click **Save**.

## Editing a Role

**To change parameters of an existing role, follow the steps below:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Roles** tab.
3. In the users list left-click at the target role.
4. Click  **Edit role**.
5. In the opened window change role attributes. Flag (unflag) the privileges you want to assign (unassign) to the role.

> **Note:**
>
> To expand / collapse privileges list, click ▶ or ◢ accordingly.

6. Click **Save**.

### Deleting a Role

**To delete role:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Roles** tab.
3. In the users list left-click at the target role.
4. Click  **Delete role**.

> **Note:**
>
> To delete several roles at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>** ) and click **Delete role**.

5. In the opened window click **Yes**.

> **Note:**
>
> You can change any role except for **Administrator** and **Security officer**.

## 3.3.3 Visibility Scopes

Visibility scope allows to perform additional access control to intercepted objects. Visibility scope is created from intercepted objects attributes. User will only see those events, which attributes match the attributes, configured in visibility scope.

For example,

User officer 1 has visibility scope with Person Ivan and Tag 1. In this case user officer 1 can only view events with the participation of Ivan and tagged 1.

> **Note:**
>
> There can be serveral scopes for one user.

Assigning visibility scope to user is described in "Creating Visibility Scope to User".

Configuring the visibility scopes list is performed in **Administration -> Users and Roles** section, **Scopes** tab.

In the working area there are list of scopes, toolbar and drop-down menu.

In the list of scopes user scopes are displayed.

Toolbar contains set of tools to work with visibility scopes.

Drop-down menu defines number of scopes to be displayed on the page.

Visibility scope attributes are listed in the following table:

| Attribute | Description |
|---|---|
| *Name* | Name of the visibility scope |
| *Description* | Note for visibility scope |

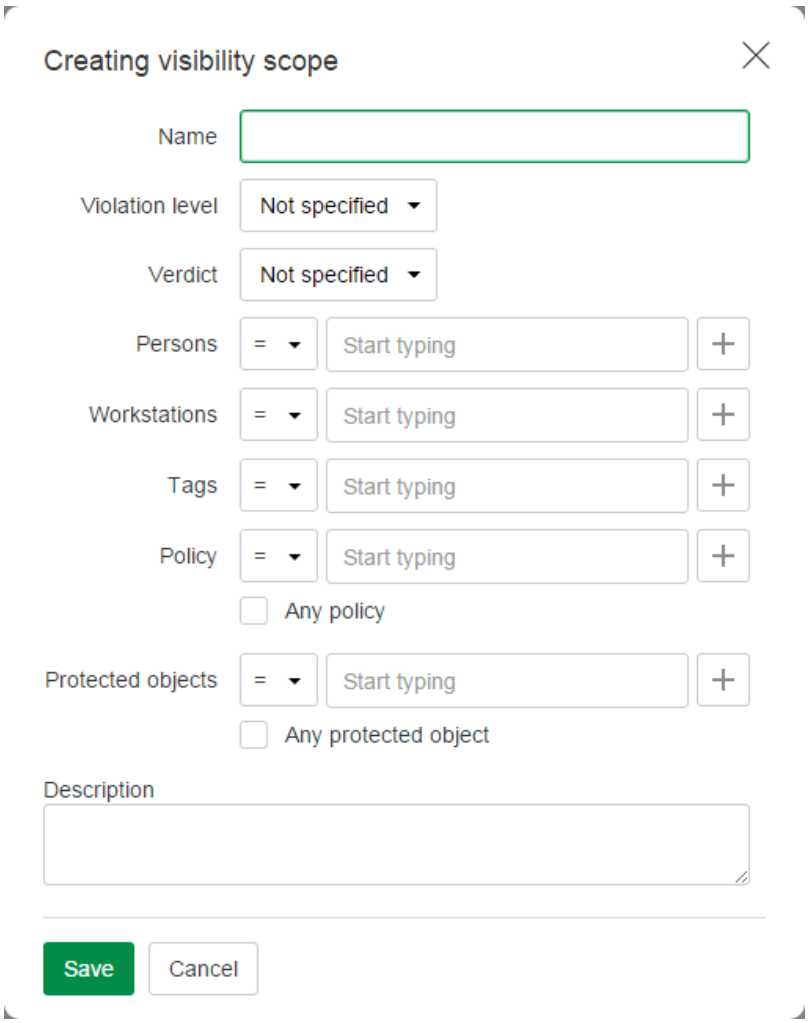
You can perform the following actions while managing visibility scopes:

- *Creating Visibility scope*;
- *Editing Visibility scope*;
- *Deleting Visibility scope*.

## Creating Visibility scope

To create a visibility scope:

1. Go to the **Administration -> Users and Roles** section, and open the **Scopes** tab.
2. Click  **Create scope**.




**Picture 5. Creating visibility scope**

3. In the opened window, specify parameters of the visibility scope:
    a. *Name* - enter name in the field.
    b. *Violation level* - choose from drop-down menu.
    c. *Verdict* - choose from drop-down menu.
    d. *Persons* :
    enter first symbols of user name and choose required value from drop-down menu
    or
    press + and set flag for the required users in the user list. Press **Add**.
    e. *Workstations* – as in item d.
    f. *Tags* - as in item d.
    g. *Policy* – as in item d.
    h. *Protected objects* – as in item d.
    i. *Any protected object* - choose option.
    j. *Description* - enter description text in the filed.

4. Click **Save**.

### Editing Visibility scope

**To edit visibility scope:**

1. Go to the **Administration -> Users and roles** section.
2. Go to the **Scopes** tab.
3. Click  **Edit scope**.
4. In the opened window change visibility scope attributes like when creating the scope (see ' Creating visibility scope').
5. Click **Save**.

### Deleting Visibility scope

**To delete visibility scope**

1. Go to section the **Administration -> Users and roles** section.
2. Go to the **Visibility scopes** tab.
3. On the toolbar click  **Delete scope**.

> **Note:**
>
> To delete several visibility scopes at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>**) and click **Delete**.

4. In the opened window click **Yes**.

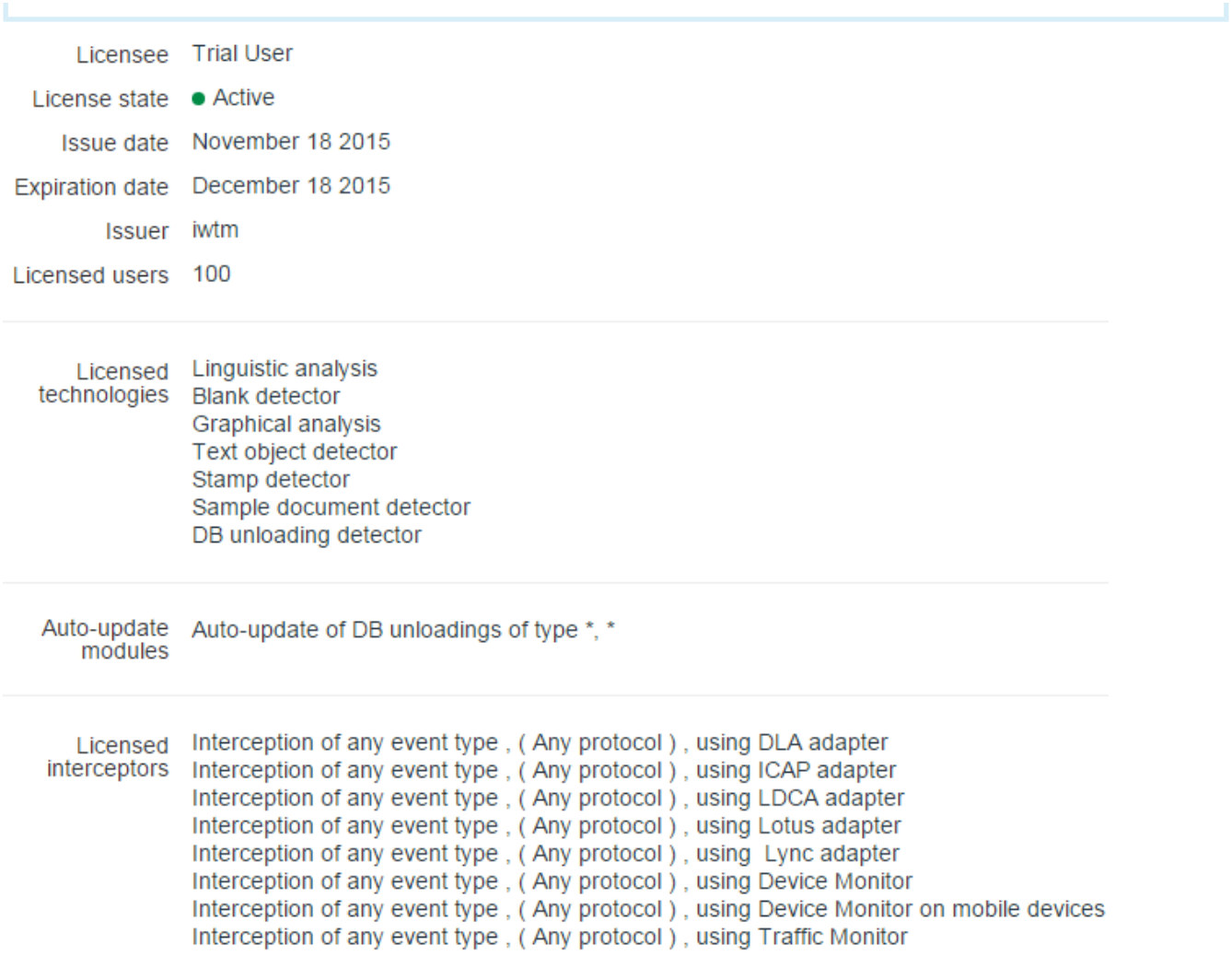
## 3.4 Managing Licenses

> **Warning!**
>
> System licensing is described in "Licensing".

License managing is being performed in **Administration –> Licenses**:

- In the left side of the working area you can see license list and license managing panel.
- In the right side of the work area you can see information about chosen licenses.

> **Note:**
>
> Editing a license in not available. You can only upload a new license or delete the old one.




You can perform the following actions with licenses:

- Installing a License;
- Deleting a License;
- Requesting a License.

## 3.4.1 Checking License Validity

Information about licensed technologies and interceptors, state, expiration date and number of licensed users, are available in **Administration –> Licenses**.

**To check license validity:**

1. Go to **Administration -> Licenses**.
2. Make sure, that **Expiration date** contains future date.
3. Make sure, that **Licensee** field value matches Licensee parameter of **license.conf** configuration file, located in `/opt/iw/tm5/etc` directory.

## 3.4.2 Installing a License

**To install a license:**

1. Go to **Administration -> Licenses**.
2. Click  **Add license** on the toolbar.
3. Click **Upload** in the pop-up menu.
4. Choose required license.lic file and click **Open** in the dialog box.
   Information about licenses and licensed technologies and interceptors will be shown in the **License adding** pop-up window.
5. Click **Add**.
6. Click **Yes** in the dialog box.

Browser page will be refreshed and new license will be added to the list. You may leave or remove the expired licenses at your option.

### 3.4.3 Deleting License

**To delete license:**

1. Choose the target license from the list.
2. On the toolbar click  **Delete**.

   > **Note:**
   >
   > To delete several several licenses at a time, select them in the list (for example, by holding **<SHIFT>** or **<CTRL>**) and click **Delete**.

3. In the opened windows press **Yes**.

### 3.4.4 Requesting a License

**To request a license:**

1. Go to **Administration** - **Licenses**;
2. On the toolbar, press  **Request license**.
3. Send an automatically formed email, adding description, if necessary.

## 3.5 Healthcheck

You can monitor the state of each server on which the System is deployed in the Management Console, in **Administration**->**Healthcheck** section.

For each server that is used in the System, indicators are listed in the table:

| | Parameter | Details |
|---|---|---|
| ● | Current System load | OK - load average: 0.21, 0.15, 0.19 |
| ● | Number of active users | USERS OK - 3 users currently logged in |
| ● | State of local mail server | SMTP OK - 0.013 sec. response time |
| ● | System time deviation | NTP OK: Offset -0.01090276241 secs |
| ● | Errors in the alert log. | OK - no errors found in log |
| ● | Size of database alert log. | OK - size of PostgresSQL system log is 9047 bytes |
| ● | State of PostgreSQL database. | OK - database postgres (0.003083 sec.) |
| ● | Server availability | PING OK - Packet loss = 0%, RTA = 0.06 ms |
| ● | Free space in root partition | DISK OK - free space: / 96362 MB (71% inode=98%): |
| ● | State of time syncronization service | OK - ntpd (pid 2491) is running... |
| ● | State of Syslog service | OK - 'rsyslogd' is running |
| ● | Server availability via SSH | SSH OK - OpenSSH_5.3 (protocol 2.0) |
| ● | Swap usage | SWAP OK - 77% free (6145 MB out of 8015 MB) |
| ● | Queue of processing actions specified in policies applied to the events. | OK - Blackboard queue: 0 item(s), 0.000 MBytes |
| ● | Number of errors occurred when processing actions from policies applied to events. | OK - Blackboard-errors queue: 0 item(s), 0.000 MBytes |
| ● | Presense of memory dumps | OK |
| ● | State of System components | OK |
| ● | Number of errors occurred when indexing events by INDEXER service. | OK - index_error queue: 0 item(s) |
| ● | TM_PG_INDEXER_QUEUE | OK - index_queue queue: 0 item(s) |
| ● | Queue for loading to storage | OK - DB queue: 0 item(s), 0.000 MBytes |
| ● | Queue processing errors | OK - Errors queue: 0 item(s), 0.000 MBytes |
| ● | Queue processing mail traffic | OK - SMTP queue: 0 item(s), 0.000 MBytes |
| ● | Number of errors occurred when processing events by IW_LOADER and IW_XML2LIR... | OK - XML2LIRO-errors queue: 0 item(s), 0.000 MBytes |
| ● | Number of running processes | PROCS OK: 283 processes with STATE = RSZDT |
| ● | Free space in /var partition | DISK OK - free space: / 96361 MB (71% inode=98%): |

For each indicator, the following information is displayed:

- **State** – the current value of the indicator:
  - ● – CRITICAL, the parameter value is higher than the critical threshold;
  - ● – WARNING, the parameter value is a warning zone (if this zone exists);
  - ● – OK, the parameter value is normal.
- **Parameter** – indicator name.
- **Details** – detailed information on healthcheck results.

> **Warning!**
>
> If the indicator value cannot be obtained, it is assumed, that current value is higher, than critical threshold.

Values are refreshed:

- Every 5 minutes – for parameters:
  - DB Alert Log Errors
  - Swap usage
  - DB Alert log Size
- Every 10 minutes – for parameters:
  - SSH availability
  - Database Status
  - Oracle TNS Status
- Every 360 minutes – for **NTP time deviation** parameter

- Every 30 minutes – for all other parameters

To refresh the values manually, **Refresh**.

### 3.5.1 Configuring notifications

**To configure notifications on theSystem state:**

1. Go to **Administration** - **Healthcheck.**
2. Click **Configure notifications** button.
3. Select **Enable notifications** option.
4. Set values for the following parameters:

| Parameter | Description |
|---|---|
| *Email server* | IP address or DNS name of the mail server, which will be used for sending notifications. You need to specify the server that supports sending messages without SMTP authentication |
| *Email port* | Email server port. Default value: `25` |
| *Email prefix* | Postal prefix is used for easy sorting of mail messages from different monitoring systems. The entered value will be added to the header of outgoing email messages. Default value: `IWTM` |
| *Recipients* | Email address of recipient/recipients. Default value: `nagios@localhost` |

5. Click *Send test message* to verify settings.
6. Click **Save**.

## 3.6 Managing Services

System Administrator can manage services without using Linux command line.

The following actions with services are possible:

- Running Service;
- Stopping Service;
- Restarting Service;
- Saving Service Logs.

### 3.6.1 Running service

**To start service**:

1. Go to **Administration - Services**.

2. Set flag in the field of the service you want to start.
3. Click button.

> **Information:**
>
> To restart several services at a time, set flag opposite each of them.

### 3.6.2 Stopping service

**To stop service**:

1. Go to **Administration - Services**.
2. Set flag in the field of the service you want to stop.
3. Click button.

> **Note:**
>
> To stop several services at a time, set flag opposite each of them.

### 3.6.3 Restarting service

**To restart service**:

1. Go to **Administration - Services**.
2. Set flag in the field of the service you want to restart.
3. Click button.

> **Note:**
>
> To restart several services at a time, set flag opposite each of them.

### 3.6.4 Saving service logs

To save service logs:

1. Go to **Adminitration - Services**.
2. Click **Save** in **Logs** column opposite the service which logs you want to save.

# 3.7 Collecting the Diagnostic Data

Collecting diagnostic data is being performed in **Administration -> Collecting the diagnostic data** section.

| Data collection mode | Description |
|---|---|
| Normal | System log information, configuration information, initial installation data |
| Extended | System log information, configuration information, initial installation data, information about system processes' crash |

Diagnostic information is being collected from the following sources:

| Data type | Path to files |
|---|---|
| Logs | `/var/log/infowatch/*.log`<br>`/var/log/nagios/nagios.log`<br>`/root/iwsetup-install-logs/*`<br>`/var/log/nagios/status.dat` |
| When Oracle DBMS is installed | `/home/oracle/addm/logs/*`<br>`/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log` |
| When PostgreSQL DBMS is installed | `/u01/postgres/pg_log/*` |
| Configuration informatuin | `/opt/iw/tm5/etc/*.conf`<br>`/opt/iw/tm5/etc/scripts/*.lua`<br>`/opt/iw/tm5/etc/config/vademecums/*.info`<br>`/opt/iw/tm5/etc/config/vademecums/vademecum.list`<br>`/etc/nagios/*`<br>`/etc/nagios/objects/*` |
| Logs and initial system installation scripts | `/root/iw*` |

**To download report on the latest diagnostics results:**

1. Go to **Administration - Collecting the diagnostic data**.
2. Download the archive by clicking **Results of the latest diagnostics are available** in `dd-mm-yyyy_hh-mm-ss` format

**Warning!**

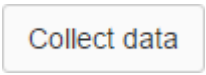
In case diagnostics has not been performed earlier, the option will not be available.

Diagnostics data can be collected in the following ways:

- Collecting the Diagnostic Data in Normal Mode;
- Collecting the diagnostic Data in extended Mode.

### 3.7.1 Collecting the diagnostic Data in normal Mode

**To collect the diagnostic data in extended mode**:

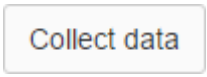
1. Go to **Administration - Services**.
2. Press 

.
3. Mark the **Normal** filed.
4. Click 

button.
5. Wait till completion of diagnostic information collection.
6. In pop-up window click **Result of the last data collection** is available in `dd-mm-yyyy_hh-mm-ss` format .

### 3.7.2 Collecting the diagnostic Data in extended Mode

**To collect the diagnostic data in extended mode**:

1. Go to **Administration - Collecting the diagnostic data**.
2. Click 

button.
3. Set marker in **Extended** field.
4. Press 

.
5. Wait till completion of diagnostic information collection.
6. Download archive by clicking **Result of the last data collection is available** in `dd-mm-yyyy_hh-mm-ss format`.

## 3.8 User Actions Audit

vThe system provides ability to monitor user actions in Management Console.

Audit events and searching filters review is being performed in **Administration -> Audit**.

The system records and displays the following information:

- logging in the System and out of the system;

- access control objects management (Users, Roles, Visibility Scope);
- user actions concerning system objects (queries, reports, policies, classifier elements and so on).

> **Note:**
>
> Changing elements through configuration cancellation is not being tracked in audit events. In this case only configuration cancellation event will be created.

**To set storing period for audit events**:

1. Go to **Administration -> Audit**;
2. Specify number of days to store audit events in **During storage of audit events (days)** area;

Working with audit events is described in the following subsections:

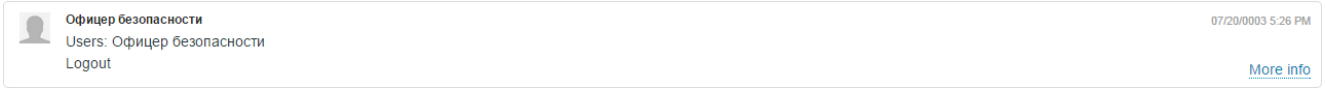
- Audit Events;
- Filtering by User;
- Filtering by Action;
- Filtering by Object;
- Filtering by Date.

## 3.8.1 Audit Events

Audit Events area is located in **Administration - Audit**.

**Audit Events** area displays **Search filters** results and represents list of audit events panels with the following attributes:

| Attribute | Description |
|---|---|
| *User* | Name of the user, which performed an action |
| *Object* | Name of an object, connected with an action |
| *Action* | Type of action, performed by user |
| *Action date and time* | Date/time of user registered action |
| *More info* | Additional information on audit event |




**Picture 1. Audit event panel**

**To filter audit events by date:**

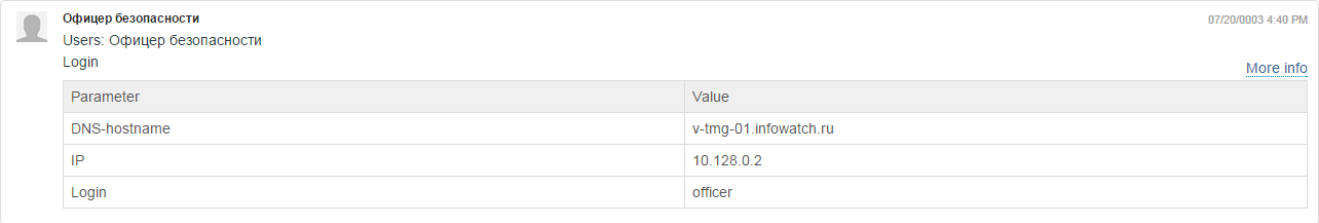
1. Go to **Administration - Audit**;
2. In the upper left corner click **Sorting** ▲ by date .

## More info

**More info** will be displayed depending on the *Object* and *Action* registered in the System.

For example, logging out of the System, one will see the following Audit parameters:

- **DNS-hostname** - name of the computer, logging out of the System;
- **IP** - IP-address of logging out computer;
- **Login** - name of the user logging out of the System.




**Picture 2. More info**

> **Warning!**
>
> Audit events parameters can be different depending on *Object* and *Action*.

**To view more information about audit event:**

1. Go to **Administration - Audit**.
2. On event panel click **More info**.

## 3.8.2 Filtering by User

**To filter events by user:**

1. Go to **Administration** - **Audit**;
2. In **Search filters** area choose user from **User** drop-down list (see "Managing System Users and their Roles").

For more filtering options, use *Action*, *Object* and *Date* parameters.

## 3.8.3 Filtering by Action

**To filter events by action:**

1. Go to **Administration** - **Audit**;
2. In **Search filters** area choose action from **Action** drop-down list.

For more filtering options, use *User*, *Object* and *Date* parameters.

### 3.8.4 Filtering by Object

**To filter events by Object**:

1. Go to **Administration** - **Audit**;
2. In **Search filters** area choose object from **Object** drop-down list.

For more filtering options, use *User*, *Action* and *Date* parameter.

### 3.8.5 Filtering by Date

**To filrer events by date:**

1. Go to **Administration** - **Audit**;
2. In **Search filters** area click on **Date** field.
3. In calendar specify dates of period.
4. Click **Apply**.
5. Click **Clear** to cancel filering by date.

For more filtering options, use *User*, *Action* and *Object* parameter.

## 3.9 Integrity monitoring

Integrity monitoring is intended to monitor system foles state. Primary reference amount is being automatically generated by the System.

System files integrity monitoring is described in the following sections:

- Manual integrity monitoring;
- Automatic integrity monitoring;
- Accepting result as standard.

### 3.9.1 Manual integrity monitoring

**To check system files integrity:**

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area click **Scan files**.

> **Note:**

In the process of integrity check the **Integrity check is being performed** message is being displayed. Upon check completion, you will see the message with date and time of the last check.

### 3.9.2 Automatic integrity monitoring

**To configure system files automatic integrity monitoring:**

1. Go to **Administration - Integrity monitoring**;
2. In the central part of the working area enable **Automatic check** setting.
3. In the **Schedule** field set the time of integrity check using **up** and **down** arrows.
4. Click **Save**.

### 3.9.3 Accepting result as standard

**To accept result of integrity check as standard:**

1. Go to **Administation - Integrity monitoring**;
2. In the central part of the working area click **Accept result as standard**.

## 3.10 Plugins

System uses plugins to connect additional interceptors. Extention allows to recieve events from external interceptors as well as automatically update sample tables.

Any API/Public API external systems connectiors should be registered in TM by adding new plugin.

Plugin is an archive in .zip format, which contains:

- **licenses** folder, which contains license files;
- **icon** folder, which contains icons for registered contacts and event types (not compulsory);
- **manifest.json** file, which contains information about plugin. File structure would be different for plugins, used for envent-recieving and sample tables update plugins.

**Note:**

Name of the files in plugin should contain only latin alphabet symbols and/or numbers.

For external system - source of events, **manifest.json** should contain the following information:

| Name | Is compulsory | Description |
|---|---|---|
| Version | Yes | Plugin version |

| Name | Is compulsory | Description |
|---|---|---|
| Developer company ID | Yes | Matches company name in License |
| Used preinstalled event types, contacts and protocols | No | List of preinstalled events type and protocols, which are being intercepted using this plugin |
| Name | Yes | Plugin name |
| Description | No | Plugin description |
| "Preinstalled" attribute | No | Whether it comprises the System |
| Registered event types. contacts and protocols | No | Contains the following data:<br>• Type of registered events with service type indication;<br>• Protocols;<br>• Actions;<br>• Code of interceptor type for InfoWatch plugin;<br>• Event type names localization at least in one language;<br>• Type of registered contacts and localization at least in one language;<br>• File with icons of registered contacts and event types. |
| Unique identifier | Yes | Unique 128-bit plugin identifier (UUID) |

For external system - source of sample tables, **manifest.json** should contain the following information:

| Name | Is compulsory | Description |
|---|---|---|
| Version | Yes | Plugin version |
| Developer company ID | Yes | Matches company name in License |
| Name | Yes | Plugin name |
| Updated data type | Yes | List of sample tables, which are being updated with the help of this plugin, with identification of source system |
| Description | Yes | Plugin description |
| "Preinstalled" attribute | No | Whether it comprises the System |

| Name | Is compulsory | Description |
|---|---|---|
| Unique identifier | Yes | Unique 128-bit plugin identifier (UUID) |

In **Plugins** sections the following actions are possible:

- Adding plugin;
- Deleting plugin;
- Working with tokens.

> **Warning!**
>
> Plugins and tokens are deleted from System when deliting DB scheme (see "Infowatch Traffic Monitor 6.0. Installation guide", article "Deleting the Database Scheme"). To reestablish Device Monitor plugin:
>
> 1. Create **/opt/iw/tm5/www/backend/protected/runtime/first_run** file using **iwtm** user;
> 2. Restart **iw_kicker** process:
>
> ```
> service iwtm restart kicker
> ```
>
> It is required to add other plugins manually (see "Adding plugin").

## 3.10.1 Adding plugin

**To add plugin:**

1. Go to **Administration - Plugins**;
2. In **Plugins** are press .
3. Press **Add**.
4. Review plugin's description and press **Install**.

> **Note:**
>
> To update plugin, add renewed version.

## 3.10.2 Deleting plugin

**To delete plugin:**

1. Go to **Administration - Plugins**;
2. In **Plugins** are press .

3. Press **Yes** to confirm deletion.

## 3.10.3 Working with tokens

Token is designed to authorize an external Push API/Public API System. After plugin has been added, token is being created automatically. (see "Adding plugin").

Token for InfoWatch Device Monitor is created automatically and is available in Administration **-> Plugins -> Tokens** section of Management console.

The following actions with tokens are possible:

- Adding token;
- Deleting token;
- Editing token data;
- Updating token value;
- Copying token.

### Adding token

**To add token:**

1. Go to **Administration** - **Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Press  .

> **Note:**
>
> Token value is generated automatically upon token creation and can be defined by user.

### Deleting token

**To delete token:**

1. Go to **Administration** - **Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Press  .

### Editing token data

**To edit token data:**

1. Go to Administration - Plugins;
2. Choose plugin in **Plugins** area;
3. Go to **Tokes** tab;
4. `By double-clicking the left mouse button in the` *`Name`* `column or` *`Description`* `type in the neccesary data.`

### Updating token value

In case token is compromised or there is a likehood, that it leaks to third-parties, w e need to generate a new token value.

**To update tokem value:**

1. Go to **Administration - Plugins**;
2. Choose plugin in **Plugin** area;
3. Go to **Tokens** tab;
4. Click  .

### Copying token

**To copy token value to the clipboard:**

1. Go to **Administration - Plugins**;
2. Choose plugin in **Plugins** area;
3. Go to **Tokens** tab;
4. Click
   
   .

# Configuring Crawler Interceptor

Crawler subsystem of InfoWatch Traffic Monitor system enables revision of the files located in corporative network for purpose of checking if the violate corporate security policies. Therefore Crawler subsystem allows to control company file resources for revelation and prevention of cases of confidential data illegal usage.

Crawler subsystem operates as one of Traffic Monitor interceptors.

The following InfoWatch Traffic Monitor components are involved to the Crawler operation:

- Crawler is a program package providing general functions executing. It 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
- Database – Crawler uses InfoWatch Traffic Monitor DB schema for storing objects considered as violations and data on scanning tasks.
- InfoWatch Traffic Monitor Management Web-Console: Crawler management is available in **Crawler** section.

> **Warning!**
>
> In case Crawler scanner and server are located in different domains or working groups, one needs to disable using encrypted connection. For more information see article "Выключение шифрования трафика между компонентами".

See detailed information on the Crawler configuration in following sections:

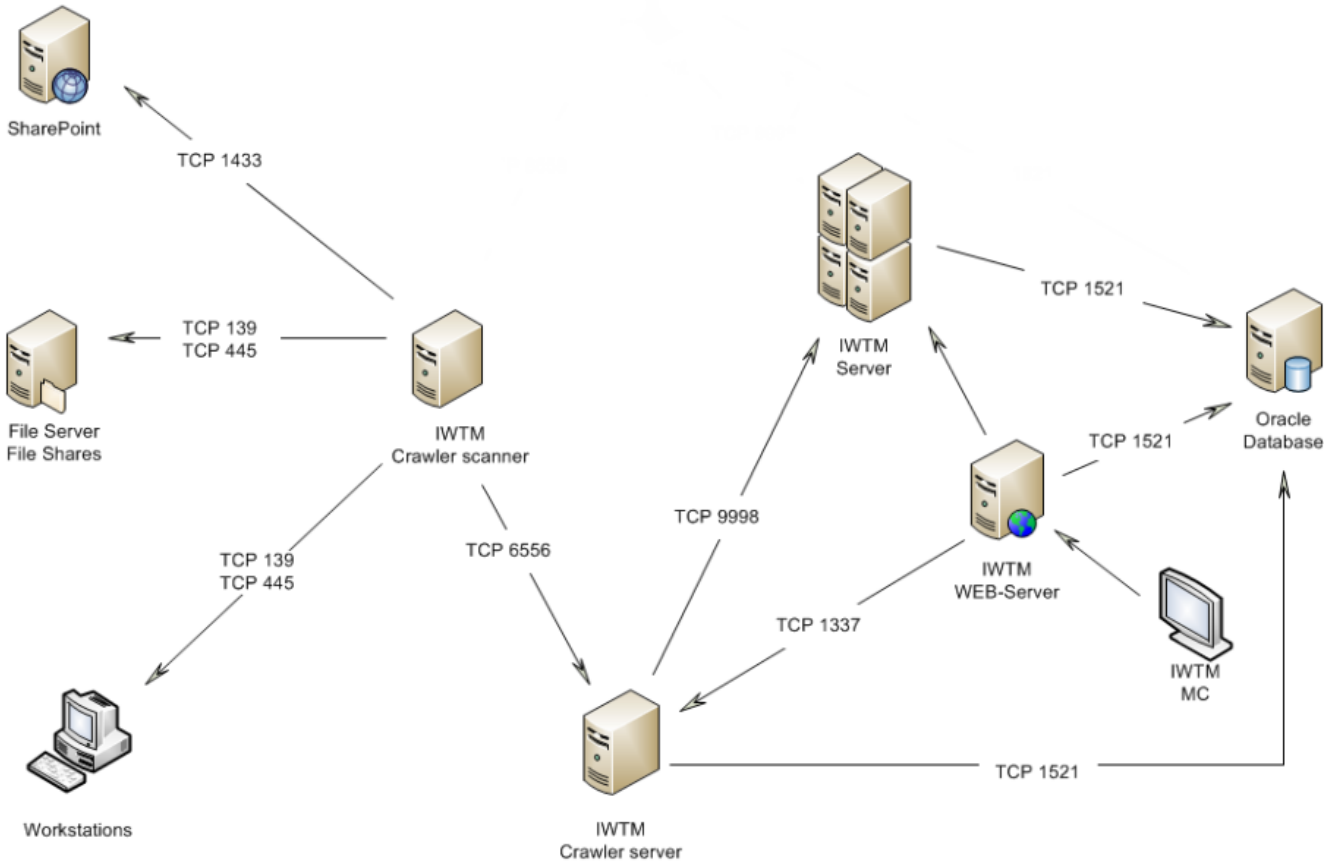
- *Configuring Network Access*;
- *Crawler Configuration Files*;
- *Crawler Log Files;*
- *Automatic deletion of Crawler events*.

# 4.1 Configuring Network Access

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

Detailed information on network ports which should be available for efficient system operation, see at the following schema and explanations table.

> **Note:**
>
> The schema does not display connection ports:
>
> - Management web-console to IWTM web-server;
> - IWTM web-server to IWTM server.
>
> Ports are not stated as when installed with kickstart all specified System components are installed to the single computer.




| Connection | Port |
|---|---|
| Crawler scanner – Crawler server | TCP 6556 |
| Crawler server – IWTM DB | TCP 1521 |
| Crawler server – IWTM | TCP 9998 |
| IWTM web-server– Crawler server | TCP 1337 |
| Crawler scanner – workstations and file servers | TCP 139<br>TCP 445 |
| Crawler scanner – SharePoint file storage (MS SQL server) | TCP 1443 |

If any system components belong to different domain controllers, then the Domain Trust setting for controllers is needed. However the remoteness of the Crawler scanner from scanned objects can significantly increase a network load. That's why we recommend you to deploy a computer with Crawler scanner in the network segment nearest to scanned segments.

**Warning!**

If you configuring the network inside the domain, the firewall should be disabled for domain as well as for domain profile.

**To turn off the firewall in the domain profile settings:**

1. Go to **Start -> Control Panel -> Windows Firewall**.
2. Choose **Advanced settings** in the left part of appeared window.

   > **Note:**
   >
   > If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

3. Choose **Windows Firewall Properties** in the central part of **Windows Firewall with Advanced Security** window.
4. Choose **Off** in the drop-down list **Firewall state**.
5. Click **OK**.

# 4.2 Crawler Configuration Files

Administrator maintaining the system can perform some low-level settings of Crawler components in configuration files:

- **Crawler server** – InfoWatch.Crawler.Server.exe.config. Located in the same directory as executed file InfoWatch.Crawler.Server.exe (default – C:\Program Files\InfoWatch\Crawler\Server for 32-bit systems and C:\Program Files (x86) \InfoWatch\Crawler\Server for 64-bit systems). See details in "Configuration File of Crawler Server".
- **Crawler scanner** – InfoWatch.Crawler.Scanner.exe.config. Located in the same directory as executed file InfoWatch.Crawler.Scanner.exe (default – C:\Program Files\InfoWatch\Crawler\Scanner for 32-bit systems and C:\Program Files (x86) \InfoWatch\Crawler\Scanner for 64-bit systems). See details in "Configuration File of Crawler Scanner".

Configuration files can be viewed and edited by any text or XML editor. File encoding is UTF-8.

## 4.2.1 Configuration File of Crawler Server

Administrator maintaining the system can perform some low-level settings of Crawler server Crawler in configuration file InfoWatch.Crawler.Server.exe.config. Configuration file is located in the same directory as executed file InfoWatch.Crawler.Server.exe (default - `C:\Program Files\InfoWatch\Crawler\Server` for 32-bit systems and `C:\Program Files (x86) \InfoWatch\Crawler\Server` for 64-bit systems).

The configuration file can be viewed and edited by any text or XML editor. File encoding is UTF-8.

Primary settings configuration is performed during Crawler installation (see “InfoWatch Traffic Monitor. Installation Guide” document).

Further the settings to change are described. Other settings are strongly recommended not to change.

- **Database connection string**. If settings of connection to the Oracle DB with used IWTM schema were changed, in `<connectionStrings>` section, `CrawlerEntities` setting, make corresponding changes in `connectionString` value.
- **Password of IWTM database schema owner’s account**, used for connection to DB. If the password was changed, specify new password in `<appSettings>` section:

```
<add key="NewDbPassword" value="new_password" />
```

Then save modified file `InfoWatch.Crawler.Server.exe.config` and restart Crawler service. New password will be encoded and saved as a value of `DbPassword` setting. `NewDbPassword` setting will be reset.

> **Note:**
>
> If you need to change an account used for server start, then prior to first server service starting enter DB password to the `NewDbPassword` field as encoded password can be decoded only by user encoded it. See more details in "Changing Account Used for Crawler's Service Start ".

- **Numbers of ports used for scanner and TM Management Console to Crawler server**. Those parameters are specified in <userSettings> section, parameters ScannerPort and ConsolePort. Values are specified in the following manner:

```
<value>port_number</value>
```

## Changing Account Used for Crawler Server's Service Start

To change account used for starting the Crawler server’s service:

1. At the computer where Crawler server works, in the list of Windows services, find **iw_crawler_server** service and stop it.
2. In the server configuration file `InfoWatch.Crawler.Server.exe.config` (see details in " Configuration File of Crawler Server"), in `NewDbPassword` setting enter a password of IWTM schema owner account, used for database connection. Save modified configuration file.
3. Return to i**w_crawler_server** service and call it **Properties** (**Actions -> Properties** or select it in the context menu opening by right-click at the service string). At the **Log On** tab specify settings of account used for starting the Crawler server’s service.
4. Run server’s service.

### SharePoint scanning scripts

Scanning SharePoint by network scanner is being performed through SQL-query to SharePoint database with preset parameters . In the new versions of scanner scripts can be changed.

By default scripts are located in folder `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts`.

**To update scripts:**:

1. In folder `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts` replace the old scripts with new ones.
2. Restart **InfoWatch Crawler Server Service** service .

> **Note:**
>
> In case scanning scripts have been changed in-service and it is required to transfer changes to the new version:
>
> 1. Save changed scripts.
> 2. Perform System update.
> 3. In folder `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts` replace scripts with the those, which have been saved earlier.
> 4. Restart **InfoWatch Crawler Server Service** service.

## 4.2.2 Configuration File of Crawler Scanner

Crawler scanning service configuration file InfoWatch.Crawler.Scanner.exe.config is located in the same directory as InfoWatch.Crawler.Scanner.exe executable file (by default - C:\Program Files \Infowatch\Crawler\Scanner\ for 32-bit system and C:\Program Files (x86)\Infowatch\Crawler\Scanner for 64-bit system). Configuration file can be viewed and edited with the help of any text or XML-editor. UTF-8 encoding file.

If necessary, System admisintrator can change the following parameters:

- Crawler server connection string. This parameter is located in the following block:
  ```
  <client>
  <endpoint name="ScannerEndpoint" binding="netTcpBinding" bindingConfiguration="
  EncryptedBinding" address="net.tcp://localhost:6556/Scanner" contract="InfoWatch.
  Crawler.Contracts.Server.IScannerDispatcher"/>
  </client>
  ```
  When changing Crawler server location, you can specify the neccessary **IP-address and server name** instead of specified `localhost` value.

- File transfer to database. This parameter is specified in the following block:
  ```
  <setting name="SendEmptyFileToTm" serializeAs="String">
  <value>False</value>
  </setting>
  ```
  If it is required for Crawler to synchronize hash with database, change `value` parameter to `True` .
- SID Resolution. This parameter is specified in the following block:
  ```
  <setting name="ResolveSIDs" serializeAs="String">
  <value>True</value>
  </setting>
  ```
  If it is required to disable SID resolution, change `value` parameter to `False`.
- Limitation of maximum number of recievers. This parameter is specified in the following block:
  ```
  <setting name="UserLimitInExpandedGroup" serializeAs="String">
  <value>0</value>
  </setting>
  ```
  Groups do not disclose with `0` value.
- Limitation of maximum number of recievers when disclosing the group. This parameter is specified in the following block:
  ```
  <setting name="UserLimitInExpandedGroup" serializeAs="String">
  <value>0</value>
  </setting>
  ```
  При значении `0` группы не раскрываются.

To apply settings, restart scaner service in Control panel -> Administration -> Services.

It is highly not recommended to change other parameters.

### 4.2.3 Выключение шифрования трафика между компонентами

This page has not yet been translated to English.

# 4.3 Crawler Log Files

System administrator can receive information about work of the scanner and Crawler server from log files, which are located in directories C:\Program Files\Infowatch\Crawler\Scanner\Logs and C:\Program Files \Infowatch\Crawler\Server\Logs for 32-bit system and C:\Program Files (x86) \Infowatch\Crawler\Scanner\Logs for 64-bit system, as well as C:\Program Files (x86) \Infowatch\Crawler\Scanner\Logs for 32-bit system and C:\Program Files (x86) \Infowatch\Crawler\Server\Logs for for 64-bit system.

**Manging Crawler logging level**

The logging level is configured in configuration files (see " Crawler Configuration Files ") .

Logging level by default is `Error`. To change logging level:

1. In <specialSources> section for three `listeners` parameters, please comment the highest string and uncomment the lowest;
2. In `switchValue` parameter specify the necessary logging level.
   For example, All:
   ```
   <allEvents switchValue="All" name="All Events">        <listeners>         <!--<add name="Rolling Flat File Trace Listener"/>->         <add name="Flat File Trace Listener" />        </listeners>
   ```
   Logging levels (listed in order of reducing details):
   `All, Verbose, Information, Warning, Error, Critical, Off`.

## 4.4 Automatic deletion of Crawler events

System is deleting objects to which no TM policy or protection object has been applied by default. To save such objects, disable deletion setting:

1. Conntect to TM server.
2. In `/opt/iw/tm5/etc/scripts/` catalogue open **system.lua** configuration file.
3. Comment the following code lines:
   ```
   if get_monitor(root) == 'CRAWLER' and
   root:xFind('/root/processing[count(postanalysis/*|policies/policy)>0]').count == 0

   then
           -- RM: Do not delete objects with analysis errors

   if root:xFind('//object/processing/messages/message[@module="cas"][@severity="fatal" or @severity="error"]').count =  0 then
   processing:find_or_add_child('delete_content'):set_text('true');
   end
   end
   ```
4. Save changes.

# Monitoring

InfoWatch Traffic Monitor Monitoring subsystem is implemented based on Nagios app that enables remote hosts & network services state monitoring.

Monitoring subsystem exercises the following functions:

- Monitoring operations of all servers (both physical and virtual) included in InfoWatch Traffic Monitor solution;
- Monitoring of all software components (OS, DBMS, DB, processes etc.) included in InfoWatch Traffic Monitor solution;

- Control of indicator values for each server and component. Here by control we mean regular retrieval of indicator value and comparing this indicator value to a threshold value. For more details on indicators, see "Healthcheck";
- Enabling or disabling monitoring of specific indicators or servers;
- Sending email notifications when indicator values exceed the normal range.

The Monitoring subsystem is autoinstalled during InfoWatch Traffic Monitor server installation by the **kickstart** program. For more details on the installation see *«InfoWatch Traffic Monitor. Installation and Configuration Guide»* document.

If InfoWatch Traffic Monitor system is deployed in such a way that all the server components (both database server and TM servers) are located at one computer (**All-in-one**) or DB server (**DB server**) is installed separately from Traffic Monitor (**Node server**), then monitoring subsystem will function without any additional settings.

In the case of more than one Traffic Monitor (**Node server**), it is required to perform additional settings (see "Configuring indicators manually")

Monitoring is being performed as well by System administrator (see "Healthcheck")

# 5.1 Monitoring Subsystem for Distributed Architecture

> **Warning!**
>
> If InfoWatch Traffic Monitor system is deployed in such a way that all the server components (both database server and TM servers) are located at one computer (**All-in-one**) or DB server (**DB server**) is installed separately from Traffic Monitor (**Node server**), then monitoring subsystem will function without any additional settings.

To perform a diagnostic of all servers included to the solution, system administrator should make some additional settings:

- Configuring Connection to Device Monitor;
- Configuring Indicators Manually;
- Configuring Addresses of Time Synchronization Server for Monitoring Subsystem;
- Configuring Threshold Value for Load Indicator;
- Configuring Notifications.

## 5.1.1 Configuring Connection to Device Monitor

To configure connection to Device Monitor server:

1. Edit **/etc/nagios/iwmon/iwmon-hosts-dm.cfg** file:
   - Uncomment `host` and `hostgroup` sections.

- In `address` parameter of `host` section define host name or IP-address of Device Monitor server.

2. In `/etc/nagios/iwmon/iwmon-services-dm.cfg` file uncomment `service` section.
3. In `/etc/nagios/iwmon/iwmon-commands.cfg` file uncomment `Check Dm server` section.
4. Restart nagios process:
   `service nagios restart`

### 5.1.2 Configuring Indicators Manually

Enabling and disabling indicators is being performed in the following file of the `/etc/nagios/iwmon` directory:

- iwmon-services-db-psql.cfg – Postgre SQL indicators configuration;
- iwmon-services-db.cfg – Oracle indicators configuration;
- iwmon-services-dm.cfg – Device Monitor indicators configuration;
- iwmon-services-loadavg.cfg – Server load parameters configuration (System load indicator);
- iwmon-services.cfg – main indicator configuration;
- iwmon-services-queue.cfg – queues indicators configuration;
- iwmon-services-traffic.cfg – subnets traffic indicator configuration;

The service_description parameter displays each indicator purpose.

To enable indicator, change `register` parameter value to `1`.

To enable indicator, change `register` parameter value to 0.

To apply changes, restart nagios:

```
nagios service restart
```

### 5.1.3 Configuring Addresses of Time Synchronization Server for Monitoring Subsystem

To provide correct time synchronization, IP address of NTP server should be specified at every system server. You may use any exact time service utilizing NTP protocol and available from your network: both network equipment and Windows domain controllers.

**To configure time synchronization at the server:**

1. Open **iwmon-services-ntp.cfg** file for editing.
2. In the check command parameter replace default IP-address with the actual IP-address of NTP server (time synchronization server).

### 5.1.4 Configuring Threshold Value for Load Indicator

Adjust activation threshold values based on number of cores on Traffic Monitor Server in **/etc/nagios /iwmon/iwmon-services-loadavg.cfg** file for Current Load indicator (service) that checks up values for load average on Traffic Monitor server.

For instance, for 4-core processor the threshold values should be specified as follows:

iwmon_check_load!10.0,8.0,6.0!20.0,16.0,12.0

Threshold values for a different number of cores are calculated proportionally.

### 5.1.5 Configuring Notifications

Monitoring subsystem enables sending email notifications where the current indicator value exceeds the threshold value.

In this section:

- Configuring Notifications on Indicators Threshold Exceeding;
- Configuring Sending Notification Mails via Postfix.

## Configuring Notifications on Indicators Threshold Exceeding

**To configure sending email notifications:**

1. In the **/etc/nagios/private/resource-notify-iw.cfg** configuration file, specify a value of the `$USER10$` parameter: a Postfix server embedded in Traffic Monitor and the port being used. For example: : `$USER10$=localhost:25`
2. In the **/etc/nagios/iwmon/iwmon-contacts.cfg** configuration file, add contacts to send notifications to. For this, add the following section for each contact:

```
define contact{
        contact_name                    <contact name>
        use                             generic-contact
        alias                           Recipient Notification
        service_notification_commands   iw-notify-service-by-email
        host_notification_commands      iw-notify-host-by-email
        email                           <address>
        register                        1
}
```

> **Note:**
>
> In this section, you can also specify additional options for sending notifications such as sending time or events for which notifications should be sent. For more information, please refer to Nagios documentation.

3. In the `members` field of the same file, specify names of contacts to which notifications will be sent. Contacts are separated by commas:

```
define contactgroup{
        contactgroup_name           admins
        alias                       IW Nagios Notification Recipient
        members                     <contact name>, <contact name1>
}
```

4. Restart Nagios with the following command:

```
service nagios restart
```

Notifications will contain the following information:

- Indicator name
- Name of server where controlled indicator exceeds the threshold value
- IP address of this server
- Current status of the indicator
- Date and time when the indicator threshold value was exceeded
- System message from source

**To set up e-mail notifications sending only for selected indicators:**

1. Go to the Nagios subsystem directory:
   `cd /etc/nagios/iwmon`
2. Open **iwmon-services.cfg** configuration file:
   `nano /etc/nagios/iwmon/iwmon-services.cfg:`
3. To identify the needed indicator, take note of the `service_description` field.
4. In the indicator section set the `notifications_enabled` parameter to:
   - 1 – to enable notifications sending
   - 0 – to disable notifications sending
5. Save changes.

> **Note:**
>
> If the notifications_enabled parameter is absent in the configuration file, you can add it manually.

## Configuring Sending Notification Mails via Postfix

If the System has the following configuration:

- SMTP-messages are sent via Postfix (see "*InfoWatch Traffic Monitor. Installation Guide*", “*System Deployment Schemas and choosing installation type*” chapter)

and

- Monitoring subsystem is located at the same server as Postfix,

then for correct sending of notification mails you should:

1. In `/etc/postfix/transport` file add the following strings:
   example@example.com smtp:[mailserver]
   where `example@example.com` is an address to send mails to and mailserver is the name of company's mail server.
   A separate string should be specified for each recipient.

   > **Warning!**
   >
   > For InfoWatch-supported projects including email address monitoring@infowatch.com is mandatory.

2. Run the command:
   `postmap /etc/postfix/transport`
3. Add transport_maps setting in the **/etc/postfix/main.cf** file:
   `transport_maps = hash:/etc/postfix/transport`
4. Restart Postfix:
   `service postfix restart`

# Administrating Database

This chapter contains information on administrating:

- *Oracle;*
- *Postgre SQL*.

Information on DB statistics collection is available in the article "DB statistics collection".

## 6.1 Oracle

This chapter contains instructions on Oracle administration:

- Routine Database Maintenance;
- Tablespaces in InfoWatch Traffic Monitor database;
- Managing Daily Tablespaces;
- Database Backup.

### 6.1.1 Routine Database Maintenance

> **Warning!**
>
> Do not power DB server off with power button: in certain cases this may cause the DB corruption.

When doing routine database maintenance, you must follow the established order:

Close all instances of the Management Console. Make sure that all connections of other programs to DB Traffic Monitor schema are closed; if there're any active connections, disable them.

1. Stop all TM processes on Traffic Monitor server:
   ```
   service iwtm stop
   service php-fpm stop
   service nginx stop
   ```
2. Retrieve list of scheduled jobs from database server. For this purpose run the following query in sqlplus using schema owner account:
   ```
   select JOB_NAME, STATE
   from user_scheduler_jobs u
   where u.enabled = 'TRUE'
   ```
3. Disable jobs by running the following script:
   ```
   BEGIN
   dbms_scheduler.disable('JOB_1',true);
   …
   dbms_scheduler.disable('JOB_N',true);
   COMMIT;
   END;
   /
   ```
   where `JOB_1… JOB_N` are the names of tasks to disable.
4. To make sure that none of these jobs is running run the following query:
   ```
   SELECT job_name
   FROM user_scheduler_running_jobs
   A list of active jobs displays. If any of the jobs is running you may run the query
   to stop it:
   BEGIN
   dbms_scheduler.stop_job('job_name');
   COMMIT;
   END;
   /
   ```
5. Make all the necessary operations with the database.

6. After all required operations are made check connection to database server from Traffic Monitor server:
   `sqlplus db_login/db_password@tns_name`
   Here `db_login` and `db_password` are the name and password of the database schema owner, and `tns_name` is the name of TNS service.
   If the test is successful, the following SQL *Plus prompt will be displayed in response to the command:
   SQL>
7. Run the processes of the Traffic Monitor server:
   ```
   service iwtm stop
   service php-fpm stop
   service nginx stop
   ```
8. Check if the system log contains errors. The path to the system log:
   `/var/log/messages`
9. If the system log contains any error messages, consult technical support service.
10. Enable running previously disabled jobs:
    ```
    BEGIN
    dbms_scheduler.enable('JOB_1',true);
    …
    dbms_scheduler.enable('JOB_N',true);
    COMMIT;
    END;
    /
    ```
    where `JOB_1… JOB_N` are the names of previously stopped jobs.

## 6.1.2 Tablespaces in InfoWatch Traffic Monitor database

There are two types of tablespaces (TS) in InfoWatch Traffic Monitor database:

| The type of tablespace | Purpose |
|---|---|
| Main | Storing the settings that are needed for the analysis and processing of the objects (configuration, tags, colors, etc.).<br>Managing the System using the Management Console (roles, user accounts, etc.) |
| Daily | Storing objects, intercepted within one day.<br>Storing information on the results of the analysis and processing of the objects (analyzed object categories, terms, etc.)<br>Consists of three tablespaces: for storing objects with states *Violation*, *No Violations, Other (tablespace to save screenprints).* Therefore the possibility of divided archiving, restoring and deleting is acquired. |

All data about the objects intercepted on a particular day are in the same daily TS. Daily TS are being created every day in such a way that the database always has TS for the next six days. The following name is automatically assigned for all daily TS:

- *<SchemaOwner>_YYYY_MM_DD_N* – tablespace for day, which contains objects without violations.
- *<SchemaOwner>_YYYY_MM_DD_V* – tablespace for day, which contains objects with violations.

Settings to manage data segments are defined when configuring database schema; however they can be changed after the schema is created "Managing Daily Tablespaces").
Using installation type **TM Standard**, events are being saved in one tablespace. Automatic calculation of free space for future events with old events deletion takes place every week. To save specific events in database, one can assign tag *Protection from deletion*. In this case event will not be deleted automatically (for more information see *InfoWatch Traffic Monitor. User Guide*).

## 6.1.3 Managing Daily Tablespaces

This section covers:

- Configuring Location of Files within File System;
- Archiving Daily Tablespaces;
- Restoring Daily Tablespaces;
- Deleting Daily Tablespaces.

### Configuring Location of Files within File System

The daily tablespaces can be stored in the same directory or distributed to various directories on various disks.

The kickstart installation program (see "*InfoWatch Traffic Monitor. Installation Guide*") sets the usage of one daily tablespace located in `/u02/oradata/`.

> **Note:**
>
> For tablespace archives, the `/u02/arch` directory is used.

However at high loads, it is recommended to place daily TS on different I/O devices (LUN, physical drives) for sequential usage. For example, when 3 file systems are defined, data is located as follows:

First day – the daily tablespace is created in File system 1.

Second day – the daily tablespace is created in File system 2.

Third day – the daily tablespace is created in File system 3.

Fourth day – the daily tablespace is created in File system 1.

…

Distribution of daily TS files (number and locations) of daily TS files can be managed using scripts.

**An example of the script to change the number of dedicated daily TS storage locations:**

```
BEGIN
```

```
pkg_part.set_df_path_cnt('4');
COMMIT;
END;
/
```

> **Warning!**
>
> After changing the number of daily TS storage locations make sure to adjust (add/delete) their location paths.

**An example of the script to change the location paths for daily TS:**

```
BEGIN
pkg_part.set_df_path('/test1/', 1);
pkg_part.set_df_path('/test2/', 2);
pkg_part.set_df_path('/test3/', 3);
pkg_part.set_df_path('/test4/', 4);
COMMIT;
END;
/
```

> **Note:**
>
> It is advisable to add “/” symbol in the end whenever specifying the path.

**An example of viewing daily TS content:**

```
select a.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) || '-' ||
power(10, trunc(log(10, a.text_size)) + 1) size_range,
count(1) cnt, sum(a.text_size) text_size
from
(
select t.tbs_name, o.service_code,
case
when length(o.text) > 0 then length(o.text)
else 1
end text_size
from object o
inner join object_source os on os.object_id = o.object_id
inner join tbs_list t on o.tbs_id = t.tbs_id
```

```
) a
group by a.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) || '-' ||
power(10, trunc(log(10, a.text_size)) + 1)
order by 1, 2, 3
```

Service code definition is specified in **services.xml** file, which is located in `/opt/iw/tm5/etc/compendiums/` catalogue.

> **Note:**
>
> To receive intercepted objects volume analysis along with DB service information, use SQLDeveloper

## Archiving Daily Tablespaces

To free some space on hard drive, you can periodically archive outdated data. It is recommended to place data archive on external devices. Data can be recovered when necessary.

> **Warning!**
>
> If the months or years are used as the time interval, it is recommended to use the maximum value of the interval in calculations. For a month - 31 days. For a year - 366 days. For example, to remove the daily TS older than 4 years specify the interval 366 * 4 = 1464 days in the IWTM_DELETE_TABLESPACES job

You can regularly archive obsolete data to free some space on a hard drive. We recommend you to save an archive with data to external data carrier. If necessary, you can restore the data.

The archiving can be performed:

- Automatically after the specified period is expired (see "Automatically Archiving of Daily Tablespaces");
- Manually – for archiving the selected daily tablespaces (see "Manual Archiving of Daily Tablespaces").

## Automatic Archiving of Daily Tablespaces

Before strating automatic archiving, check, that archiving catalogue has been set properly:

```
select value
from setting
where setting = 'archive_path'
```

`Orcale` user should be an owner of the catalogue.

In case catalogue has been set improperly, reset it, using the following command:

```
begin;
```

```
select sp_setting_set('archive_path', '/test/archive/');

commit;
```

To perform TS archiving automatically (by default the function is disabled) you can use the following scripts (run under the account of the database schema owner):

- For daily TS storing objects with *Violation* status:

```
begin
sp_setting_set('violation_archive_enabled', 1);
sp_setting_set('violation_archive_period', D);
commit;
end;
```

where:
1 – indicates that authomatical deletion is enabled (to disable specify 0 instead);
D – is a number of days at the end of which the daily TS will be archived by the System.

- For daily TS storing objects with *No Violation* status:

```
begin
sp_setting_set('noviolation_archive_enabled', 1);
sp_setting_set('noviolation_archive_period', D);
commit;
end;
```

where:
1 – indicates that automatical deletion is enabled (to disable specify 0 instead);
D – is a number of days at the end of which the daily TS will be archived by the System.

## Manual Archiving of Daily Tablespaces

Manual archiving of daily tablespaces is performed in the following steps:

**Selecting daily tablespaces and data files**

To get a list of disconnected tablespaces, you must run the following query to the database under the account of the database schema owner. The queries are built according to the archiving policy of your company. For example, to select the daily TS storing the objects which were intercepted more than 100 days ago, run the following query:

```
SELECT t.tbs_id, t.tbs_name, t.part_date

FROM tbs_list t

WHERE t.part_date<trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (0, 3)
```

> **Warning!**
>
> It is strongly recommended to run the following sample query in this section in order to retrieve the list of files. This is due to the fact that the file list if generated by any other ways may be incomplete.

In this case, the following query is created to select data files:

```
SELECT f.file_name
FROM dba_data_files f
WHERE f.tablespace_name in
(
  SELECT t.tbs_name
  FROM tbs_list t
  WHERE t.part_date<trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (0, 3)
)
```

where `t.status IN (0, 3)` indicates that the tablespaces with the *ReadWrite* (status code `0`) and *ReadOnly* (status code `3`) statuses are selected for archiving.

### Disconnecting Daily Tablespaces from the Database

> **Warning!**
>
> It is strongly recommended not to disable daily TS when the IWTM_ADD_PARTS, IWTM_DELETE_TABLESPACES and IWTM_ARCHIVE_TABLESPACES jobs are running as it may cause the data loss.

1. Call the procedure on behalf of the owner of the database schema, call the procedure:

   ```
   begin
   IWTM.pkg_part.archive_tablespace(N);
   end;
   ```

   where `N` is a value of tbs_id attribute of the target TS from the `tbs_list` table.
   `After running this script status of daily TS will change to Offline.`
2. Repeat the procedure call for each daily TS you want to disable.

### Moving Datafiles

Transfer the data files belonging to the disabled daily TS to the other data carrier.

To get a list of data files for all disconnected tablespaces, use the following script:

`select tbs_name from tbs_list` where `NOTE = 'Tablespace is offline'`

where `tbs_name` is a name of a tablespace.

`tbs_list` is a name of a table.

Data files are stored in the catalogue:

`select value from setting where setting = 'archive_path'.`

## Restoring Daily Tablespaces

> **Warning!**
>
> A tablespace can only be restored in the database schema, from which it was disconnected (even if this schema was updated). The restoration of the tablespace after total database schema reinstallation is impossible.

#### Moving data files

To restore daily TS, you must move data files of this tablespace from a data carrier to the folder which path you can obtain using the following command:

```
select value from setting where setting = 'archive_path'
```

> **Warning!**
>
> Make sure that the *oracle* user has reading and writing privileges for the directory to move the data files to.

#### Connecting the daily tablespace

> **Warning!**
>
> Do not connect daily TS during IWADDPARTS, IWTM_DELETE_TABLESPACES jobs. This may cause the data loss.

1. On behalf of the owner of the database schema, call the procedure:
   ```
   begin
   pkg_part.restore_tablespace(N);
   end;
   ```
   where `N` is ID of the tablespace (specified in tbs_list).
   After procedure ending the status of TS will change to *Restored*.
2. Repeat the procedure call for each daily TS you want to enable.

## Deleting Daily Tablespaces

If you do not need to further store the data, you can use the procedure for deleting daily TS ( **IWTM_DELETE_TABLESPACES**). The procedure automatically deletes all the data in a tablespace, segments, and also the tablespace and data files.

> **Warning!**

1. Deleting tablespaces cannot be undone. If you complete the operation, you will not be able to restore the deleted data.
2. After removal of the tablespaces disconnected from the database (with *Offline* status), the data files will be kept. To free space on your hard drive, delete these files manually.
3. IWTM_DELETE_TABLESPACES job cannot operate tablespaces which were disconnected/connected manually

As a result, this procedure will remove all the daily TS (and including information about the archived daily TS), which satisfy the following condition:

*The date of creating a tablespace is less or equal to the difference between the current date and the specified time interval for deleting the tablespace.*

> **Note:**
>
> If the archived daily TS cannot be restored (because the information in it was removed from the database), then you can delete the data files of the daily TS from the archive.

While the tablespaces are being deleted, the **iw_deliverd**, **iw_dbloader**, **iw_updater** daemons are automatically stopped. When the deletion procedure is completed, the processes will be automatically restarted. It is recommended to run the job to delete data on a daily basis. Otherwise, the amount of deleted data increases, which in turn increases the time for running the procedure and consequently increases the idle time of the Traffic Monitor Server.

> **Warning!**
>
> If months or years are used as a time interval, then we recommend you to apply the maximal interval value in the counting: 31 days for a month and 366 days for a year. For example, to delete daily TS older than 4 years, specify 366*4=1464 days interval in the IWTM_DELETE_TABLESPACES job.

**Setting the interval of daily TS deletion**

To perform TS deletion automatically (by default the function is disabled) you can use the following scripts (run under the account of the database schema owner):

- For daily TS storing objects with *Violation* status:

```
begin

sp_setting_set('violation_delete_enabled', 1);

sp_setting_set('violation_delete_period', D);

  commit;

end;
```

where:

1 indicates that authomatical deletion is enabled (to disable specify 0 instead);

D is a number of days at the end of which the daily TS will be deleted by the System.

- For daily TS storing objects with *No Violation* status:

```
begin
  sp_setting_set('noviolation_delete_enabled', 1);
  sp_setting_set('noviolation_delete_period', D);
  commit;
end;
```

where:

1 indicates that automatical deletion is enabled (to disable specify 0 instead);

D is a number of days at the end of which the daily TS will be deleted by the System.

#### Enabling procedure autorun according to schedule

By default, automatic deletion of daily TS is disabled. To enable the deletion of daily TS according to schedule (every day at 00 h 30 min 00 s), run the following script under the account of the database schema owner:

BEGIN

```
dbms_scheduler.enable('IWTM_DELETE_TABLESPACES ');
COMMIT;
END;
```

/

To disable procedure autorun, run the following script:

```
BEGIN
dbms_scheduler.disable('IWTM_DELETE_TABLESPACES');
COMMIT;
END;
```

/

#### Manual run

If you need an immediate launch of procedure for deletion of daily TS (e.g., due to file system space shortage the interval of deletion was changed, but the next launch of the job will not happen soon), run the following script:

```
BEGIN
dbms_scheduler.run_job('IWTM_DELETE_TABLESPACES');
END;
```

/

### 6.1.4 Database Backup

To minimize the risk of data loss we strongly recommend to backup the database on a monthly basis. We recommend you to use dedicated storage system for backups storage.

Experienced Oracle database administrators can perform a backup at the running database (“hot backup”) using Oracle-recommended RMAN program (see Oracle documentation), previously taken the Oracle database to ARCHIVELOG mode.

For non-database administrators who do not have standard backuping methods we recommend creating a “cold backup” at the stopped database. This procedure may also be used to migrate the database from one server to another.

This section further covers:

- Creating Database Backup;
- Restoring the Database from the Backup.

## Creating Database Backup

Creating database backup (cold backup procedure) is performed in the following order:

- Defining the Size of Backup;
- Checking the Backup Storage;
- Creating Backup Directories;
- Creating Recovery Aid Files;
- Collecting a List of Files to Backup;
- Stopping IWTM System;
- Stopping Oracle Database;
- Copying database Files to the Backup Storage.

## Defining the Size of Backup

**To define backup size:**

1. Log the computer that hosts database, as **oracle** user.
2. Open Oracle SQL*Plus and log as **sysdba**:
   ```
   OS> sqlplus / as sysdba
   ```
3. If the system was installed using kickstart, you can use **wsqlplus** command.

> **Note:**
>
> `wsqlplus` command is an alias of `sqlplus`:
>
> ```
> alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'
> ```

Wait for **Connected** message.

4. Copy (or enter) the following SQL queue to the command prompt:
   ```
   SQL> SELECT ROUND(SUM(bytes)/1024/1024/1024,4) GB FROM ( SELECT SUM(bytes) bytes
   FROM dba_data_files union SELECT SUM(bytes) bytes FROM dba_temp_files union SELECT
   SUM(bytes) bytes FROM v$log);
   ```
5. Note the resulted database size.
6. Exit Oracle SQL*Plus:
   ```
   SQL> exit
   ```

## Checking the Backup Storage

**Check your backup storage. It should confirm the following requirements:**

- Located outside the computer where database is running.
- Available from the computer where backuping servers and database are located.
- Free space at the hard disk is bigger than backup size.

**To define the hard disk free space**

Run the command as **root**:

```
OS> df -h
```

Make sure this number is bigger than database size.

## Creating Backup Directories

> **Warning!**
>
> Backup directories should be located at computer other than the database is located.

1. Log the system as **root** user.
2. Create the directory for backup files storage:
   ```
   OS> mkdir /opt/IWTM_Backup_Files
   ```
3. Create subdirectories:
   ```
   OS> mkdir /opt/IWTM_Backup_Files/Oradata
   OS> mkdir /opt/IWTM_Backup_Files/IWTM
   OS> mkdir /opt/IWTM_Backup_Files/Recovery_Aid
   ```
4. Grant permissions to these directories to the **oracle** user:
   ```
   OS> chmod 777 /opt/IWTM_Backup_Files/ -R
   ```

## Creating Recovery Aid Files

To provide database restoring, besides data files, you need recovery aid files: a **trace** file of the control file and a copy of the **init.ora** file.

The **trace** file of the control file contains the names and locations of all of the data files and additional data files that have been added to the database. It also contains the redo logs and the commands that can be used to recreate the database structure.

The **init.ora** file contains Oracle initializing parameters, including the names and locations of the database control files.

**To create trace file of the control file, spfile file and to backup them:**

1. Log on to the computer that hosts the Oracle database as the **oracle** user.
2. Open Oracle SQL*Plus and log as **sysdba** user:
   `OS> sqlplus / as sysdba`
   If the system was installed using kickstart, you can use **wsqlplus** command.

   > **Note:**
   >
   > `wsqlplus` command is an alias of `sqlplus`:
   >
   > `alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'`

   Wait for **Connected** message.
3. Copy (or enter) the following SQL queue to the command prompt:
   `SQL> alter database backup controlfile to trace;`
4. To find the directory in which the trace file was created, enter:
   `SQL> show parameter user_dump;`
   At that folder you can find **trc** file and **alert_iwtm.log** file (alert_INSTANCE_NAME). At log file you can find the name of the trace file which was created.
   Exit Oracle SQL*Plus:
   `SQL> exit`
5. If the system was installed using kickstart and default parameters were left, you can check last **alert_iwtm.log** records by the following command:
   `OS> tail -f /u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log`
   Press CTRL+C to exit view.
6. Create a copy of **spfile** (**pfile**):
   `OS> sqlplus / as sysdba`
   `SQL> CREATE PFILE from SPFILE;`
7. To find the directory in which the pfile file was created, enter:
   `SQL> show parameter PFILE`
   It returns a path to the directory where pfile was created (/u01/app/oracle/product/db_1/dbs/ by default).

In this folder the **initiwtm.ora** file is located too. Please create a backup for **initiwtm.ora** file.
Exit Oracle SQL*Plus:
`SQL> exit`

8. Copy trace and spfile files to the backup storage, to previously created `/opt/IWTM_Backup_Files/Recovery_Aid` subdirectory.
9. Be sure to copy the file with the most recent date and timestamp. To check the date and the timestamps of the files in the directory, enter:
   `OS> ll`
10. Rename the file so that it can be easily identified, for example:
    `controlfilebackupMMDDYY.trc`

## Collecting a List of Files to Backup

You can create a list of files that need to be backed up. These lists are used in a later step.

1. Log on to the computer that hosts the Oracle database as the **oracle** user.
2. Open Oracle SQL*Plus and log as **sysdba** user:
   OS> sqlplus / as sysdba
   Wait for **Connected** message.
3. Create the list of directories to backup using following SQL commands:
   `SQL> SELECT file_name FROM dba_data_files UNION SELECT file_name FROM dba_temp_files UNION SELECT name FROM v$controlfile union select member name from v$logfile;`
   The output is like:

```
/u01/app/oracle/fast_recovery_area/iwtm/control02.ctl
/u01/app/oracle/oradata/iwtm/control01.ctl
/u01/app/oracle/oradata/iwtm/redo01.log
/u01/app/oracle/oradata/iwtm/redo02.log
/u01/app/oracle/oradata/iwtm/redo03.log
/u01/app/oracle/oradata/iwtm/redo04.log
/u01/app/oracle/oradata/iwtm/redo05.log
/u01/app/oracle/oradata/iwtm/redo06.log
/u01/app/oracle/oradata/iwtm/redo07.log
/u01/app/oracle/oradata/iwtm/redo08.log
/u01/app/oracle/oradata/iwtm/redo09.log
/u01/app/oracle/oradata/iwtm/redo10.log
/u01/app/oracle/oradata/iwtm/redo11.log
/u01/app/oracle/oradata/iwtm/redo12.log
/u01/app/oracle/oradata/iwtm/redo13.log
/u01/app/oracle/oradata/iwtm/sysaux01.dbf
/u01/app/oracle/oradata/iwtm/system01.dbf
/u01/app/oracle/oradata/iwtm/temp01.dbf
/u01/app/oracle/oradata/iwtm/undotbs01.dbf
/u01/app/oracle/oradata/iwtm/users01.dbf
/u02/oradata/IWTM_2012_06_25_1.dbf
```

```
/u02/oradata/IWTM_2012_06_26_1.dbf
/u02/oradata/IWTM_2012_06_27_1.dbf
/u02/oradata/IWTM_2012_06_28_1.dbf
/u02/oradata/IWTM_2012_06_29_1.dbf
/u02/oradata/IWTM_2012_06_30_1.dbf
/u02/oradata/IWTM_2012_07_01_1.dbf
/u02/oradata/IWTM_2012_07_02_1.dbf
/u02/oradata/IWTM_2012_07_03_1.dbf
/u02/oradata/IWTM_2012_07_04_1.dbf
/u02/oradata/iwtm_1.dbf
```

4. Exit Oracle SQL*Plus:
   ```
   SQL> exit
   ```

## Stopping IWTM System

Stopping IWTM system is unnecessary but recommended if IWTM server has low free space.

**To stop IWTM system**:

1. On the computer that hosts IWTM services, log on as **root** user.
2. Stop all running Traffic Monitor Server services:
   ```
   OS> service iwtm stop
   ```
3. You can start services later (when backuping finished) using the following command:
   ```
   OS> service iwtm start
   ```

## Stopping Oracle Database

> **Waning!**
>
> Please stop ORACLE database before backuping database files.

**To stop Oracle database:**

1. On the computer that hosts the database, log on as the ***oracle*** user.
2. In the command prompt, enter:
   ```
   OS> dbshut $ORACLE_HOME
   ```
3. You can start services later (when backuping finished) using the following command:
   ```
   OS> dbstart $ORACLE_HOME
   ```

## Copying database Files to the Backup Storage

1. Please make sure all Oracle services are stopped. If Oracle services are not stopped, backup files can be damaged and unusable for the restoring.

2. On the computer that hosts the database, copy directories (and their content) using previously created directories list (see "Collecting a List of Files to Backup").
   If the system was installed using kickstart and default parameters were left, the path should be as follows:
   Copy contents of **/u01/app/oracle/oradata/iwtm/** folder to **/opt/IWTM_Backup_Files/IWTM** folder
   And contents of **/u02/oradata/** folder to **/opt/IWTM_Backup_Files/Oradata** folder
3. From the computer that hosts database copy **/u01/app/oracle/product/db_1/dbs/orapwiwtm** file to **/opt/IWTM_Backup_Files/Recovery_Aid** folder of the computer where backup files are located.

## Restoring the Database from the Backup

Considering the reason of your database fail, choose appropriate recovering database procedure:

- If the database was damaged due to system failure or user fault, restore old database. For example, if any essential file was occasionally deleted, you can restore the database to the state when this file existed: see "Restoring at the Same Database".
- If old database cannot be used any more, create a new one and recover data there: see "Restoring at the New Database".

## Restoring at the Same Database

This is the procedure of restoring to the database having the same directory structure as the one the backup was created at.

**To restore the database by creating a new one:**

1. Make sure the database environment is healthy. Check the existing database, the database server that hosts the existing database, and the computer that hosts the database server.
2. Install Oracle database according to «*InfoWatch Traffic Monitor. Installation Guide*» document.
3. Perform the following tasks:
   a. Delete all content of **/u02/oradata/ and /u01/app/oracle/oradata/iwtm/** directories
   b. Copy the content of **/opt/IWTM_Backup_Files/Oradata/** directory to **/u02/oradata/** directory
   c. Copy the content of **/opt/IWTM_Backup_Files/IWTM/** directory to **/u01/app/oracle/oradata/iwtm/** directory
   d. Rename **control01.ctl** file located in **/opt/IWTM_Backup_Files/Oradata/** directory to **control02.ctl** and copy it to **/u01/app/oracle/flast_recovery_area/iwtm/** directory
   e. Check permissions.
4. If necessary change them:

```
OS> chown oracle:oinstall /u02/oradata -R
OS> chown oracle:oinstall /u01/app/oracle/oradata/iwtm/ -R
OS> chown oracle:oinstall /u01/app/oracle/fast_recovery_area/iwtm/ -R
```

5. Start database:
   ```
   OS> dbstart $ORACLE_HOME
   ```

### Restoring at the New Database

If the drive structure of the new database differs from the drive structure of the old database, perform the following actions:

1. Edit the **initiwtm.ora** file in the **/opt/IWTM_Backup_Files/Recovery_Aid** directory to reflect the drive structure of the new database.
2. Copy the edited **initiwtm.ora** file to the **$ORACLE_HOME/dbs** directory on the computer that hosts the new database.
3. Log on to the computer that hosts the Oracle database as the **oracle** user.
4. Open Oracle SQL*Plus and connect as the **sysdba** user:
   ```
   OS> sqlplus / as sysdba
   ```
5. Generate spfile
   ```
   SQL> create spfile from pfile;
   ```
6. If you need to rename some files, you can use the following script:
   ```
   OS> sqlplus / as sysdba
   SQL> startup mount
   SQL> alter database rename file '/<path_to_proddb_files>/<filename1>' to '
   /<path_to_clonedb_files>/<filename1>';
   …
   SQL> alter database rename file '/<path_to_proddb_files>/<filenameN>' to '
   /<path_to_clonedb_files>/<filenameN>';
   SQL> shutdown immediate
   ```
   Here `path_to_proddb_files` is a path to the directory where new database files are located (to where backup is restoring), and `path_to_clonedb_files` is a path to the directory where backup files are located.

# 6.2 Postgre SQL

To connect to DB server from Traffic Monitor server terminal, use the following command:

```
psql postgres iwtm
```

To connect to DB from workstations running Windows, use pgAdmin program.

Connection information is located in **/opt/iw/tm5/csw/postgresql/database.conf** configuration file.

This chapter contains instructions on aministration Postgre SQL:

- Tablespaces in InfoWatch Traffic Monitor Database;
- Managing Daily Tablespaces;
- Database backup.

## 6.2.1 Tablespaces in InfoWatch Traffic Monitor database

There are two types of tablespaces (TS) in InfoWatch Traffic Monitor database:

| The type of tablespace | Purpose |
|---|---|
| Main | Storing the settings that are needed for the analysis and processing of the objects (configuration, tags, colors, etc.).<br>Managing the System using the Management Console (roles, user accounts, etc.) |
| Daily | Storing objects, intercepted within one day.<br>Storing information on the results of the analysis and processing of the objects (analyzed object categories, terms, etc.)<br>Consists of three tablespaces: for storing objects with states *Violation*, *No Violations, Other (tablespace to save screenprints).* Therefore the possibility of divided archiving, restoring and deleting is acquired. |

All data about the objects intercepted on a particular day are in the same daily TS. Daily TS are being created every day in such a way that the database always has TS for the next six days. The following name is automatically assigned for all daily TS: *<Schema Owner>_X.* Here:

- *Schema Owner*– the owner of database schema.
- *X* – number of TS (tbs_id from tbs_list table).

Settings to manage data segments are defined when configuring database schema; however they can be changed after the schema is created (see "Managing Daily Tablespaces").
Using installation **TM Standard** type, events are being saved in one tablespace. Automatic calculation of free space for future events with old events deletion takes place every week. To save specific events in database, one can assign *Protection from deletion* tag. In this case event will not be deleted automatically (for more information see "Infowatch Traffic Monitor 6.0. User Guide", article "Managing Tags").

## 6.2.2 Managing Daily Tablespaces

In this chapter:

- Archiving Daily Tablespaces;
- Restoring Daily Tablespaces;
- Configuring Location of Files in File System;
- Deleting Daily Tablespaces.

### Archiving Daily Tablespaces

To free some space on hard drive, you can periodically archive outdated data. It is recommended to place data archive on external devices. Data can be recovered when necessary.

**Warning!**

If the months or years are used as the time interval, it is recommended to use the maximum value of the interval in calculations. For a month - 31 days. For a year - 366 days. For example, to remove the daily TS older than 4 years specify the interval 366 * 4 = 1464 days in the IWTM_DELETE_TABLESPACES job.

You can regularly archive obsolete data to free some space on a hard drive. We recommend you to save an archive with data to external data carrier. If necessary, you can restore the data.

The archiving can be performed:

- Automatically after the specified period is expired (see "Automatic Archiving of Daily Tablespaces");
- Manually – for archiving the selected daily tablespaces (see "Manual Archiving of Daily Tablespaces ").

## Automatic Archiving of Daily Tablespaces

Before strating automatic archiving, check, that archiving catalogue has been set properly:

```
select value
from setting
where setting = 'archive_path'
```

`Orcale` user should be an owner of the catalogue.

In case catalogue has been set improperly, reset it, using the following command:

```
begin;
select sp_setting_set('archive_path', '/test/archive/');
commit;
```

To perform TS archiving automatically (by default the function is disabled) you can use the following scripts (run under the account of the database schema owner):

- - For daily TS storing objects with *Violation* status:
    ```
    begin;
    select sp_setting_set('violation_archive_enabled', '1');
    select sp_setting_set('violation_archive_period', 'D');
    commit;
    ```

  where:
  1 – indicates that authomatical deletion is enabled (to disable specify 0 instead);
  D – is a number of days at the end of which the daily TS will be archived by the System.

  - For daily TS storing objects with *No Violation* status:
    ```
    begin;
    select sp_setting_set('noviolation_archive_enabled', '1');
    select sp_setting_set('noviolation_archive_period', 'D');
    ```

```
commit;
```

where:
1 – indicates that automatical deletion is enabled (to disable specify 0 instead);
D – is a number of days at the end of which the daily TS will be archived by the System.

## Manual Archiving of Daily Tablespaces

Manual archiving of daily tablespaces is performed in the following steps:

**Selecting daily tablespaces and data files**

To get a list of disconnected tablespaces, you must run the following query to the database under the account of the database schema owner. The queries are built according to the archiving policy of your company. For example, to select the daily TS storing the objects which were intercepted more than 100 days ago, run the following query:

```
SELECT t.tbs_id, t.tbs_name, t.part_date
FROM tbs_list t
WHERE t.part_date < current_date - 100 + 23 / 24 AND t.status IN (0, 3);
```

> **Warning!**
>
> It is strongly recommended to run the following sample query in this section in order to retrieve the list of files. This is due to the fact that the file list if generated by any other ways may be incomplete.

Daily TS are located in separate catalogues.

To get names of these catalogues, run the following command:

```
#su - postgres -c 'psql postgres iwtm'

postgres=# \db
               List of tablespaces
    Name    |  Owner   |        Location
------------+----------+------------------------
 iwtm       | iwtm     | /u01/iwtm_main/iwtm
 iwtm_421   | iwtm     | /u01/iwtm_data/iwtm_421
 iwtm_423   | iwtm     | /u01/iwtm_data/iwtm_423
 iwtm_424   | iwtm     | /u01/iwtm_data/iwtm_424
 iwtm_425   | iwtm     | /u01/iwtm_data/iwtm_425
 iwtm_426   | iwtm     | /u01/iwtm_data/iwtm_426
 iwtm_427   | iwtm     | /u01/iwtm_data/iwtm_427
 iwtm_428   | iwtm     | /u01/iwtm_data/iwtm_428
 iwtm_429   | iwtm     | /u01/iwtm_data/iwtm_429
```

```
 iwtm_430   | iwtm     | /u01/iwtm_data/iwtm_430
 iwtm_431   | iwtm     | /u01/iwtm_data/iwtm_431
 iwtm_432   | iwtm     | /u01/iwtm_data/iwtm_432
 iwtm_433   | iwtm     | /u01/iwtm_data/iwtm_433
 iwtm_434   | iwtm     | /u01/iwtm_data/iwtm_434
 iwtm_435   | iwtm     | /u01/iwtm_data/iwtm_435
 iwtm_436   | iwtm     | /u01/iwtm_data/iwtm_436
 iwtm_437   | iwtm     | /u01/iwtm_data/iwtm_437
 iwtm_438   | iwtm     | /u01/iwtm_data/iwtm_438
 iwtm_439   | iwtm     | /u01/iwtm_data/iwtm_439
 iwtm_440   | iwtm     | /u01/iwtm_data/iwtm_440
 iwtm_441   | iwtm     | /u01/iwtm_data/iwtm_441
 iwtm_442   | iwtm     | /u01/iwtm_data/iwtm_442
 iwtm_443   | iwtm     | /u01/iwtm_data/iwtm_443
 iwtm_444   | iwtm     | /u01/iwtm_data/iwtm_444
 iwtm_445   | iwtm     | /u01/iwtm_data/iwtm_445
 iwtm_446   | iwtm     | /u01/iwtm_data/iwtm_446
 pg_default | postgres |
 pg_global  | postgres |
(28 rows)
```

Where `Name` corresponds to values from sample `select tbs_name, tbs_id from iwtm.tbs_list`.

### Disconnecting Daily Tablespaces from the Database

> **Warning!**
>
> It is strongly recommended not to disable daily TS when the *<SchemaOwner>*_iwtm_add_parts, *<SchemaOwner>*_iwtm_delete_tablespaces,*<SchemaOwner>*_iwtm_archive_tablespaces jobs are running as it may cause the data loss.

1. Call the procedure on behalf of the owner of the database schema, call the procedure:
   `select pkg_part_archive_tablespace(N);`
   where `N` is a value of tbs_id attribute of the target TS from the `tbs_list` table.
   After running this script status of daily TS will change to `Offline`.
2. Repeat the procedure call for each daily TS you want to disable.

### Moving Datafiles

Transfer the data files belonging to the disabled daily TS to the other data carrier.

To get a list of data files for all disconnected tablespaces, use the following script:

```
select value from setting where setting = 'archive_path';
```

## Restoring Daily Tablespaces

> **Warning!**
>
> A tablespace can only be restored in the database schema, from which it was disconnected (even if this schema was updated). The restoration of the tablespace after total database schema reinstallation is impossible.

### Moving data files

To restore daily TS, you must move data files of this tablespace from a data carrier to the folder which path you can obtain using the following command:

```
select value from setting where setting = 'archive_path'
```

> **Warning!**
>
> Make sure that the *postgres* user has reading and writing privileges for the directory to move the data files to.

### Connecting the daily tablespace

> **Warning!**
>
> Do not connect daily TS during *<SchemaOwner>*_iwtm_add_parts, *<SchemaOwner>*_iwtm_delete_tablespaces and *<SchemaOwner>*_iwtm_archive_tablespaces jobs. This may cause the data loss.

1. On behalf of the owner of the database schema, call the procedure:
   `select pkg_part_restore_tablespace(N);`
   where `N` is ID of the tablespace (specified in tbs_list).
   After procedure ending the status of TS will change to *Restored*.
2. Repeat the procedure call for each daily TS you want to enable.

## Configuring Location of Files in File System

The daily tablespaces can be stored in the same directory or distributed to various directories on various disks.

The kickstart installation program (see “InfoWatch Traffic Monitor. Installation Guide" document) sets the usage of one daily tablespace located in `/u02/pgdata`.

> **Note:**
>
> For tablespace archives, the `/u02/arch` directory is used.

However at high loads, it is recommended to place daily TS on different I/O devices (LUN, physical drives) for sequential usage. For example, when 3 file systems are defined, data is located as follows:

First day – the daily tablespace is created in File system 1.

Second day – the daily tablespace is created in File system 2.

Third day – the daily tablespace is created in File system 3.

Fourth day – the daily tablespace is created in File system 1.

…

Distribution of daily TS files (number and locations) of daily TS files can be managed using scripts.

**An example of the script to change the number of dedicated daily TS storage locations:**

```
begin;
select pkg_part_set_df_path_cnt('4');
commit;
```

> **Warning!**
>
> After changing the number of daily TS storage locations make sure to adjust (add/delete) their location paths.

**An example of the script to change the location paths for daily TS:**

```
begin;
select pkg_part_set_df_path('/test1/', 1);
select pkg_part_set_df_path('/test2/', 2);
select pkg_part_set_df_path('/test3/', 3);
select pkg_part_set_df_path('/test4/', 4);
commit;
```

> **Note:**
>
> It is advisable to add “/” symbol in the end whenever specifying the path.

**An example of viewing daily TS content:**

```
select a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) || '-' ||
power(10, trunc(log(10, a.binary_size + a.text_size)) + 1) size_range,
count(1) cnt, sum(a.binary_size) binary_size, sum(a.text_size) text_size
```

```
from
(
select date_trunc('day', o.capture_date) d, s.display_name code, o.object_id,
coalesce(length(os.source),0)+coalesce(length(os.context),0)+
coalesce(length(o.gui_xml),0)+coalesce(length(o.preview_data),0) binary_size,
coalesce(length(o.text), 0) text_size
from object o
inner join service s on o.service_code = s.service_id and s.language = 'eng'
inner join object_source os on os.object_id = o.object_id
where o.capture_date between to_date('05.05.2014', 'dd.mm.yyyy') and to_date
('14.05.2014', 'dd.mm.yyyy')
) a
group by a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) || '-' ||
  power(10, trunc(log(10, a.binary_size + a.text_size)) + 1)
order by 1, 2, 3
```

**Note:**

To receive intercepted objects volume analys along with DB service information, use SQLDeveloper

## Deleting Daily Tablespaces

If you do not need to further store the data, you can use the procedure for deleting daily TS ( *<SchemaOwner>*_iwtm_delete_tablespaces). The procedure automatically deletes all the data in a tablespace, segments, and also the tablespace and data files.

**Warning!**

1. Deleting tablespaces cannot be undone. If you complete the operation, you will not be able to restore the deleted data.
2. After removal of the tablespaces disconnected from the database (with *Offline* status), the data files will be kept. To free space on your hard drive, delete these files manually.
3. *<SchemaOwner>*_iwtm_delete_tablespaces job cannot operate tablespaces which were disconnected/connected manually

As a result, this procedure will remove all the daily TS (and including information about the archived daily TS), which satisfy the following condition:

*The date of creating a tablespace is less or equal to the difference between the current date and the specified time interval for deleting the tablespace.*

> **Note:**
>
> If the archived daily TS cannot be restored (because the information in it was removed from the database), then you can delete the data files of the daily TS from the archive.

While the tablespaces are being deleted, the **iw_deliverd**, **iw_dbloader**, **iw_updater** daemons are automatically stopped. When the deletion procedure is completed, the processes will be automatically restarted. It is recommended to run the job to delete data on a daily basis. Otherwise, the amount of deleted data increases, which in turn increases the time for running the procedure and consequently increases the idle time of the Traffic Monitor Server.

> **Warning!**
>
> If months or years are used as a time interval, then we recommend you to apply the maximal interval value in the counting: 31 days for a month and 366 days for a year. For example, to delete daily TS older than 4 years, specify 366*4=1464 days interval in the *<SchemaOwner>* _iwtm_delete_tablespaces job.

**Setting the interval of daily TS deletion**

To perform TS deletion automatically (by default the function is disabled) you can use the following scripts (run under the account of the database schema owner):

- For daily TS storing objects with *Violation* status:

```
begin;

select sp_setting_set('violation_delete_enabled', '1');

select sp_setting_set('violation_delete_period', 'D');

commit;
```

where:

1 indicates that authomatical deletion is enabled (to disable specify 0 instead);

D is a number of days at the end of which the daily TS will be deleted by the System.

- For daily TS storing objects with *No Violation* status:

```
begin;

select sp_setting_set('noviolation_delete_enabled', '1');

select sp_setting_set('noviolation_delete_period', 'D');commit;
```

where:

1 indicates that automatical deletion is enabled (to disable specify 0 instead);

D is a number of days at the end of which the daily TS will be deleted by the System.

**Manual run**

If you need an immediate launch of procedure for deletion of daily TS (e.g., due to file system space shortage the interval of deletion was changed, but the next launch of the job will not happen soon), run the following script:

```
select pkg_part_delete_tablespaces()
```

## 6.2.3 Database Backup

To minimize the risk of data loss we strongly recommend to backup the database on a monthly basis. We recommend you to use dedicated storage system for backups storage.

For non-database administrators who do not have standard backuping methods we recommend creating a “cold backup” at the stopped database. This procedure may also be used to migrate the database from one server to another.

This section further covers:

- Creating Database Backup;
- Резервное копирование базы данных 1.

## Creating Database Backup

Creating database backup (cold backup procedure) is performed in the following order:

- Defining the Size of Backup;
- Checking the Backup Storage;
- Creating Backup Directories;
- Stopping IWTM System;
- Copying database Files to the Backup Storage;
- Stopping Postgre SQL.

## Defining the Size of Backup

To define size of the future archive, it is necessary to find out summary size of catalogue of Postgres DB, main tablespace size and daily tablespaces catalogues:

1. Enter the system using **root**;
2. Get summary catalogue size:
   ```
   du -sx -BM /u01/postgres/ /u02/pgdata
   ```

## Checking the Backup Storage

**Check your backup storage. It should confirm the following requirements:**

- Located outside the computer where database is running.

- Available from the computer where backuping servers and database are located.
- Free space at the hard disk is bigger than backup size.

**To define the hard disk free space**

Run the command as **root**:

```
OS> df -h
```

Make sure this number is bigger than database size.

## Creating Backup Directories

> **Warning!**
>
> Backup directories should be located at computer other than the database is located.

1. Log the system as **root** user.
2. Create the directory for backup files storage:
   ```
   mkdir /opt/IWTM_Backup_Files
   ```
3. Create subdirectories:
   ```
   mkdir /opt/IWTM_Backup_Files/Pgdata
   mkdir /opt/IWTM_Backup_Files/IWTM_main
   mkdir/opt/IWTM_Backup_Files/IWTM_data
   ```

## Stopping IWTM System

Stopping IWTM system is unnecessary but recommended if IWTM server has low free space.

**To stop IWTM system**:

1. On the computer that hosts IWTM services, log on as user **root**.
2. Stop all running Traffic Monitor Server services:
   ```
   service iwtm stop
   ```
   You can start services later (when backuping finished) using the following command:
   ```
   service iwtm start
   ```

## Stopping Postgre SQL

**To stop Postgre SQL database:**

1. On the computer that hosts the database, log on as the **root** user.

2. In the command prompt, enter:
   ```
   service pgagent-9.4 stop
   service postrgesql-9.4 stop
   ```
   You can start services later (when backuping finished) using the following command:
   ```
   service pgagent-9.4 start
   service postrgesql-9.4 start
   ```

## Copying database Files to the Backup Storage

1. Please make sure all Postgre SQL services are stopped. If Postgre SQL services are not stopped, backup files can be damaged and unusable for the restoring.
2. On the computer that hosts the database, copy directories (and their content) using previously created directories list.
   If the system was installed using kickstart and default parameters were left, the path should be as follows:
   Copy contents of **/u01/iwtm_main/ and /u01/iwtm_data/** folders to **/opt/IWTM_Backup_Files/IWTM_main** and **/opt/IWTM_Backup_Files/IWTM_data** folders accordingly
   And contents of **/u01/postgres/** folder to **/opt/IWTM_Backup_Files/Pgdata** folder

## Restoring the Database from the Backup

Considering the reason of your database fail, choose appropriate recovering database procedure:

- If the database was damaged due to system failure or user fault, restore old database. For example, if any essential file was occasionally deleted, you can restore the database to the state when this file existed: see "Restoring at the Same Database".
- If old database cannot be used any more, create a new one and recover data there: see "Restoring at the New Database".

## Restoring at the Same Database

This is the procedure of restoring to the database having the same directory structure as the one the backup was created at.

**To restore the database by creating a new one:**

1. Make sure the database environment is healthy. Check the existing database, the database server that hosts the existing database, and the computer that hosts the database server.
2. Stop Postgre SQL services:
   ```
   service pgagent-9.4 stopservice postrgesql-9.4 stop
   ```
3. Install Postgre SQL database according to «InfoWatch Traffic Monitor. Installation Guide» document.
4. Perform the following tasks:
   a. Delete all content of **/u01/iwtm_main/**, **/u01/iwtm_data/** and **/u01/postgres/** directories
   b. Copy the content of **/opt/IWTM_Backup_Files/Pgdata** directory to **/u01/postgres/** directory

c. Copy the content of **/opt/IWTM_Backup_Files/IWTM_main/** directory to **/u01/iwtm_main/** directory

d. Copy the content of **/opt/IWTM_Backup_Files/IWTM_data/** directory to **/u01/iwtm_data/** directory

5. Check permissions.
   If necessary change them:
   ```
   chown postgres /u01/iwtm_main/ -R
   chown postgres /u01/iwtm_data/ -R
   chown postgres /u01/postgres/ -R
   ```
6. Start database:
   ```
   service postrgesql-9.4 start
   service pgagent-9.4 start
   ```

### Restoring at the New Database

Restoring to Postgre SQL, it is important to copy DB files to the same catalogues, in which they were initially located.

To restore DB, copy catalogues, check permissions and start DB services (see "Restoring at the Same Database")

# Administrating the Server End of InfoWatch Traffic Monitor

This chapter contains description of Traffic Monitor server part components and methods of their use:

- Traffic Monitor Server Modules and Processes;
- Setting Traffic Monitor Server End Configuration Files;
- Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file);
- Configuring Settings of Enclosures Archives Processing (extractors.conf file);
- Archiving a Mail Queue Directory;
- Logging of System Work;
- Loading an Object Queue;
- Recovering the System after Failures;
- Configuring forwarding data to SIEM;
- Deleting temporary files.

# 7.1 Traffic Monitor Server Processes

This section covers:

- List of Traffic Monitor Server End Processes;
- Using Traffic Monitor Server End Processes.

## 7.1.1 List of Traffic Monitor Server End Processes

Managing of the processes is performed by managing of the modules: the module can include a process or group of processes.

| Purpose | Process name | Process description | Configuration file |
|---|---|---|---|
| **Data collection** | iw_icap | Processes HTTP-traffic. Receives HTTP requests from the ICAP client. Extracts data from an HTTP requests. Then, the extracted data is added to the XML context. The XML context is sent to the subsystem of analysis and decision making for analysis. After analysis the response is sent to the ICAP-client to allow/deny the delivery of the HTTP-request. It also transfers HTTP-request to **iw_loader** process that saves it to the database | /opt/iw/tm5/etc /icap.conf |
| | iw_sniffer | Receives a traffic transferred by SMTP, HTTP, ICQ, POP3, IMAP protocols | /opt/iw/tm5/etc /sniffer.conf |
| | iw_proxy | Receives a copy of the traffic, separates it to HTTP-, ICQ- and SMTP-traffic and sends it to **iw_messed**. Includes the following processes:<br>• iw_proxy_http – receives a copy of HTTP- traffic.<br>• iw_proxy_icq - receives a copy of ICQ- traffic.<br>• iw_proxy_smtp - receives a copy of SMTP- traffic.<br>Each process receives the object and creates XML-context fron it. Then XML-context is transferred to the subsystem of analysis and decision making. After analysis the copy of object is delivered to the **iw_loader** process that saves is to the database | /opt/iw/tm5/etc /proxy.conf |
| | iw_smtpd | Receives SMTP-messages. When integrated with the Postfix mail server it receives incoming messages from Postfix. If there is no integration with Postfix, it receives the incoming mail from the corporate mail server or mail client (depending on the settings of your mail system). Receives incoming messages in SMTP format, converts SMTP envelope data to the XML context. Then it transfers SMTP-message and XML context to the **iw_messed** process | /opt/iw/tm5/etc /smtpd.conf |
| | iw_capstack | Performs the processing of traffic transferred by POP3 and IMAP protocols | /opt/iw/tm5/etc /capstack.conf |
| | iw_messed | | |

| Purpose | Process name | Process description | Configuration file |
|---|---|---|---|
| | | The process of mail processing. Extracts data from SMTP-, POP3- and IMAP-objects. Then extracted data is added to the XML context. The prepared XML context (containing the data extracted from the envelope and the e-mail) is transferred to the subsystem of analysis and decision making for analysis. After the analysis **iw_messed** transfers the allowed SMTP messages to the mail system component that delivers mail (only in the normal and transparent transport modes). For integration with Postfix mail server this component is Postfix. If there is no integration with Postfix, then the component depends on the settings configured in your mail system: it can be a corporate mail server or a mail client. Besides, a copy of screened SMTP message is delivered to the **iw_loader** process that saves is to the database | /opt/iw/tm5/etc/messed.conf |
| | iw_xapi | Recieves objects from Device Monitor via thrift-interface and is laid to a file queue. Then transmits objects to **iw_analysis** process. When receiving eml-objects, transmits them to **iw_messed** process | /opt/iw/tm5/etc/xapi.conf |
| | iw_analysis | Takes objects from file queue, to which objects are laid by **iw_xapi**. It transmits objects for processing to **iw_warpd**, **iw_cas**, **iw_pas**, **iw_luaengined**. Then objects are laid to file queue to be loaded to the database by **iw_loader** | /opt/iw/tm5/etc/analysis.conf |
| | iw_expressd | Processes objects from InfoWatch Device Monitor and DeviceLock<br>Upon receipt of the data (shadow copy of file or print job) from InfoWatch Device Monitor or shadow copy of file from DeviceLock Adapter **iw_expressd** creates XML-context from received object. Then, the XML context is sent to the subsystem of analysis and decision making. After analysis the shadow copy is sent to xml2liro process. Then a shadow copy is transferred to the **iw_loader** process that saves it to the database | /opt/iw/tm5/etc/expressd.conf |
| **Data processing** | iw_warpd | Manages the processes of extracting the data from containers enclosed in intercepted objects | /opt/iw/tm5/etc/warpd.conf |
| | iw_cas | Content analysis server<br>The **iw_casd** process receives queries as a plain text from the interception subsystem for content analysis. When the analysis is completed, the query result is returned to the subsystem of analysis and decision making | /opt/iw/tm5/etc/cas.conf |
| | iw_pas | Receives analysis results from **iw_cas**. Defines presence of protected objects and adds corresponding attributes to an object | /opt/iw/tm5/etc/pas.conf |
| | iw_luaengined | Provides the executing of LUA-script according to actual policy | /opt/iw/tm5/etc/luaengined.conf |
| | iw_xml2liro | Transforms xml-context received from traffic, to binary format **liro** | /opt/iw/tm5/etc/xml2liro.conf |

| Purpose | Process name | Process description | Configuration file |
|---|---|---|---|
| **Loading to DB** | iw_qmover_client | It works on the Traffic Monitor Server, installed at a branch office. Sends intercepted objects to headquarter office database | /opt/iw/tm5/etc /qmover_client. conf |
| | iw_qmover_server | It works on the Traffic Monitor Server, installed in the headquarters office. Receives objects from the client installed at the branch office. It also sends objects to the **iw_loader** process that saves it to the database | /opt/iw/tm5/etc /qmover_server. conf |
| | iw_loader | Downloads objects to the database. Receives objects (checked by subsystem of analysis and decision making) from **iw_messed**, **iw_expressd**, **iw_proxy** processes. Downloads received objects to the database | /opt/iw/tm5/etc /loader.conf |
| **Infrastructure** | iw_adlibitum | Manages the processes of receiving the relevant data from Active Directory server | /opt/iw/tm5/etc /adlibitum.conf |
| | iw_agent | Required for System configuration management | /opt/iw/tm5/etc /agent.conf |
| | iw_blackboard | Performs the interaction of applied policies and database | /opt/iw/tm5/etc /blackboard.conf |
| | iw_bookworm | Reference book for the System | /opt/iw/tm5/etc /bookworm.conf |
| | iw_config_compiler | Transforms the configuration file of Content analysis server to binary file for using the configuration in the content analysis | /opt/iw/tm5/etc /config_compiler. conf |
| | iw_configerator | Compiles configuration, which is sent to Device Monitor | /opt/iw/tm5/etc /configerator.conf |
| | iw_crawler | Supporting process for Crawler subsystem (the Crawler operates at the server different from Traffic Monitor Server) | /opt/iw/tm5/etc /crawler.conf |
| | iw_deliver | Delivers SMTP-letters to receivers if the delivery is allowed by Management Console (only in Normal and Transparent transport modes). Also delivers SMTP-letters which were not delivered by **iw_messed** process for one reason or another (for example because of no connection between mail relay-server or mail client) | /opt/iw/tm5/etc /deliver.conf |
| | iw_indexer | Indexes text of database objects. Gets access to database to index it and adds indexes to file storage. When a search query is performed, **sphinx** receives obejct ids from file storage | /opt/iw/tm5/etc /indexer.conf |

| Purpose | Process name | Process description | Configuration file |
|---|---|---|---|
| | iw_kicker | Provides WebGUI correct work, provides start of services: agent, blackboard, crawler, export, import, report, notifier, selection, systemcheck,xapisamplecompiler, samplecompiler. | /opt/iw/tm5/etc /kicker.conf |
| | iw_licensed | Licensing subsystem. Performs a monitoring and processing of licenses installed in the System | /opt/iw/tm5/etc /licensed.conf |
| | iw_notifier | Process to send System notifications | /opt/iw/tm5/etc /kicker.conf |
| | iw_report | Process for creating reports | /opt/iw/tm5/etc /kicker.conf |
| | iw_sample_compiler | Creates fingerprints from downloaded sample files | /opt/iw/tm5/etc /sample_compiler. conf |
| | iw_selection | Supporting process for working with filters (queries) | /opt/iw/tm5/etc /kicker.conf |
| | iw_serman | Registers and saves registration data of services interacting with user interface | /opt/iw/tm5/etc /serman.conf |
| | iw_system_check | Process, which collects data from Nagios service and provides received data to be displayed in Management Console | /opt/iw/tm5/etc /system_check. conf |
| | iw_updater | Loads a configuration from the database to the Traffic Monitor Server | /opt/iw/tm5/etc /updater.conf |
| | iw_whiteboard | Allows the server processes to display messages in user interface | /opt/iw/tm5/etc /whiteboard.conf |

## 7.1.2 Using Traffic Monitor Server End Processes

List of Traffic Monitor processes is presented in chapter "List of Traffic Monitor Server End Processes"

All Traffic Monitor Server processes (except for **iw_warpd**) are being launched under **iwtm** user. **iw_warpd** is being launched under **root** user.

Accounts are being created automatically during Traffic Monitor Server installation (see details in «InfoWatch Traffic Monitor. Installation Guide»).

### Note:

User name is being registered in configuration files' `User` parameter of `Permissions` section. It is not recommended to change the setting to provide stability of the System.

During the run-time Traffic Monitor Server processes status is checked by pguard script added to the /opt/iw/tm5/bin file during installation. If for any reason one or more Traffic Monitor Server processes are stopped the pguard script restarts them.

The Traffic Monitor Server processes are managed using iwtm file located in `/etc/rc.d/init.d` folder. iwtm and iw-caserv files are autorun scripts for run levels 2, 3, 4, 5.

### Note:

1. To intercept a copy of traffic using Sniffer (ICQ- HTTP-, SMTP-traffic) the separate **iw_proxy** processes are launched
2. The **iw_qmover_server, iw_qmover_client** processes are only available after installation of remote database management module. Each process is launched on the respective end (in branches – **iw_qmover_client**, in headquarter office – **iw_qmover_server**).

Start keys for **iwtm** script:

| Start key | Purpose |
|---|---|
| start | run the processes |
| stop | stop the processes |
| restart | restart the processes |
| reload | reload process configuration |
| status | view the processes status |

### Examples of commands

| Action | Command |
|---|---|
| Restart the Content Analysis subsystem processes | service iwtm restart cas |
| Verify the status for Traffic Monitor server processes | service iwtm status |
| Verify the status of the Content Analysis subsystem processes | service iw_cas status |

> **Warning!**
>
> PID-files are stored in /opt/iw/tm5/run folder. If an error occurs, you must delete it all PID files before starting the processes.

**Changing the settings of the autorun for the processes**

For each process managed by iwtm script, you can specify autorun settings in configuration file.

**To enable / disable process autorun (example for iw_sniffer service):**

1. Stop Traffic Monitor server processes:
   `service iwtm stop`
2. In **/opt/iw/tm5/etc/sniffer.conf** file:
   To enable process autorun, in the process block setup:
   `"Startup" : {"Enabled" : true}`
   To disable process autorun, in the process block setup:
   `"Startup" : {"Enabled" : false}`
3. Run Traffic Monitor server processes:
   `service iwtm start`

# 7.2 Setting Traffic Monitor Server End Configuration Files

This document subsection describes the settings of System configuration files which can be changed basing on System operation specifics for your organization. It is not recommended to edit any files which are not described in this subsection.

Configuration files are located in `/opt/iw/tm5/etc`.

There are configuration files of components used for configuration System components. For example, for configuration of **iw_loader** component **loader.conf** configuration file is used (Find full lost of configuration files in section "Specific Configurable Settings of Configuration Files").

There are common configurable settings (see "Common Configurable Settings of Configuration Files") and settings specific for each of configuration files (see "Specific Configurable Settings of Configuration Files").

## 7.2.1 Common Configurable Settings of Configuration Files

The JSON file format is used for System operation configuring. This subsection describes most used sections and settings.

> **Warning!**
>
> It is not recommended to edit any settings which are not described in this document.

Common configurable settings contain in the following sections of configuration files:

- The Logging Section;
- The Startup Section;
- The Nookdir Section;
- The Permissions Section.

## The Logging Section

The `Logging` section defines logs output.

| Setting | Description |
|---|---|
| `ActiveBackends` | Configuring log files output. Possible values:<br>• `Console` - output to the console (if the process is running not as a daemon, otherwise logs will be saved to the /dev/null directory)<br>• `Syslog` - output to the system log (/var/log/messages)<br>• `File` - output to the individual file (the directory of this file is specified in DefaultDirectory parameter) |
| `DefaultDirectory` | The path to the directory containing log files |
| `Descriptions` | Format description for each logging type and specific settings |
| `GlobalLevel` | Global level of logging. If the *warning* value is set then log will contain only messages with *warning* level and higher |
| `DisableLogging` | Possibility of total disabling of the logging for the component |

> **Note:**
>
> In case you need to debug process, use `DebugBreak` parameter. Default value is `false`. It is not recommended to edit parameter without InfoWatch employee's control.

## The Startup Section

The Startup section defines if the module autorun is enabled (true value) or disabled (false value).

> **Warning!**
>
> The enabling and disabling of iw_proxy service's modules is performed in the following way:
>
> - "Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}
> – enabling all modules;

- "Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}
  – enabling iw_proxy_http module;
- "Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}
  – disabling all modules.

### The Nookdir Section

The Nookdir section defines the work catalogue of the module. Default value is `/opt/iw/tm5`.

### The Permissions Section

The `Permissions` section defines the Linux group and user, under whose account the process is started:

| Parameter | Description |
|---|---|
| `Enabled` | The process is started under the user from a group with restricted permissions. The default value is `true`<br><br>**Note**: If you change the value to `false`, the process will be started under the **root** user without restrictions |
| `Group` | A group of Linux users, which includes the user. The default value is `iwtm`<br><br>**Note**: The user and the group are created automatically during the System installation |
| `User` | A name of the Linux user under whose account the process is started. The default value is `iwtm` |

## 7.2.2 Specific Configurable Settings of Configuration Files

The JSON file format is used for System operation configuring.

> **Warning!**
>
> It is not recommended to edit any settings which are not described in this document.

This subsection describes most used sections and parameters of the following configuration files:

- The serman_resolver.conf configuration file ;
- The sniffer.conf configuration file;
- The proxy.conf configuration file;
- The oracle.conf configuration file;
- The cas.conf configuration file;
- The expressd.conf configuration file;
- The messed.conf configuration file;
- The smtpd.conf configuration file;

- The capstack.conf configuration file;
- The indexer.conf configuration file;
- The web.conf configuration file.

## The serman_resolver.conf configuration file

The file stores supporting data for **iw_serman** module: components registration data which can be requested by other registered services.

| Setting | Description |
|---|---|
| `Host` | IP address where **iw_serman** service operates |
| `Password` | User password. Used for connecting to Serman |
| `Port` | Port for connecting to Serman |
| `Username` | User name. Used for connecting to Serman |

## The sniffer.conf configuration file

If the Traffic Monitor Management Web-Console and Sniffer component are installed at the same computer then you should add the following code to `Listenareas` section, `http` setting, `Rules` subsetting:

```
{
"HiPort": 80,
"IP": "[Server_IP]",
"LoPort": 80,
"Mask": "0.0.0.0",
"Policy": "DROP"
}
```

Here `[Server_IP]` – is IP address of the server where sniffer service is installed.

## The proxy.conf configuration file

Configuration file **proxy.conf** contains the following sections describing settings for processing copies of different types of objects received from Sniffer:

- The Http Section;
- The Icq Section;
- The Smtp Section.

## The Http Section

In the Http section there are settings for processing copies of HTTP queries and ICQ messages (when intercepting ICQ over HTTP), received from Sniffer.

| Parameter | Description |
|---|---|
| `AuthContext` | Disables the saving HTTP-requests in queue without authentication. Possible values:<br>• `0` – saves your queries without authentication;<br>• `1` – queries are not saved with "*407*" proxy response,<br>• `2` - are not saved queries with NTLM Type 1, or without *Proxy-Authorization* header. In this case the `SkipNegotiate` setting has no value set: The system functions as if the value was set to `On`.<br>The default value is `0` |
| `CharsetDetection` | Method of determining the encoding of the text. Default value is `0`. In this case, the encoding is determined by the usual method. After extraction in the context, the texts of some POST-queries may be displayed incorrectly. To fix this problem you can set value to `1` |
| `DataPoolSize` | Maximum volume of allocated memory for connection processing, in Mb. The default value is `1024` |
| `DecodeHttpContent` | Enabling the unpacking of query contents where Content-Encoding header is present with gzip, deflate or compress value. The default value is `true` |
| `DefaultCodepage` | Coding incoming ICQ-traffic. The default value is `cp1251` |
| `DialogBytesCount` | The size of dialogue (in bytes), at which the ICQ-dialog is saved in a (when intercepting the ICQ over the HTTP) file queue. The default value is `500` |
| `DialogTimeout` | The size of dialogue (in bytes), at which the ICQ-dialog is saved in a (when intercepting the ICQ over the HTTP) file queue. The default value is `5` |
| `ExtractHttpEntity` | Enabling the procedure of extracting text from the encoded content of the query by external unpackers. This procedure applies in case of failures of internal decoding procedure using zlib. The default value is `false` |
| `FakeFileTransferPort` | The port, which blocks the attempts to transfer files after redirection to it. The default value is `62225` |
| `FormatXmlContext` | Formatting XML. Used for debugging. The default value is `false` |

| Parameter | Description |
| --- | --- |
| `HttpDumpPath` | Path to dump file for HTTP-traffic |
| `IcqDumpPath` | Path to dump file for ICQ-traffic |
| `IcqFilter` | Ability to intercept ICQ-messages (if the value On is enabled), sent via proxy (over HTTP). By default the function is enabled |
| `IcqIgnoreHosts` | Disabling interception of definite hosts ICQ-sessions. |
| `IcqKnownServers` | Ranges for ICQ servers when intercepting the ICQ over HTTP. Several ranges are listed, separated by commas, for example: " `205.188.251.0/24:443, 64.12.30.0/24:443, 205.188.8.8:443` " |
| `IcqSessionTimeOut` | Time of ICQ-session inactivity in seconds, after which traffic interception stops. The default value is `10800` |
| `LogAuth` | Logging information about connecting user login to his POST-requests. The default value is `false` |
| `LogBlock` | A record in the system log of messages about blocking the intercepted HTTP-requests. The logging is enabled if the value true is specified. The logging is disabled by default – value `false` |
| `MaxMemoryBlock` | The maximum amount of POST-query (in kilobytes) that can be stored in memory. Blocks of a larger size will be loaded into temporary files. The default value is `4096` Kb |
| `MessageWindow` | The number of dialogue messages, at which the ICQ-dialog is saved in a (when intercepting the ICQ over the HTTP) file queue. The default value is `10` |
| `MinHeader` | The minimum volume of text (in bytes) for one block of variable in the URL encoding, which will be forwarded to the content analysis server. The default value is `10`. |
| `MinText` | Minimum text size to be sent to iw_cas. The default value is `0` |
| `OCR` | Using OCR technology. The default value is `false` |
| `OnlyPost` | Interception of POST-requests only. The default value is `true` |
| `SetCp1251` | Using windows 1251 charset instead of mac-cyrillic when the text encoding in HTTP request is identified automatically. The default value is false. If your software supports windows-1251 charset, it is recommended to keep the setting enabled (On value). The charset may be identified incorrectly. Specifically when Cyrillic text volume is rather small, the mac-cyrillic charset may be selected in place of windows-`1251` |

| Parameter | Description |
| --- | --- |
| `SkipNegotiate` | Disables the saving of HTTP-requests with NTLM Type 1 to the queue (necessary to eliminate duplicate queries). The default value is false. While implementing scheme of implementation, when HTTP-traffic copy is intercepted via Sniffer, it must take value `false`. |
| `SkipStat4XX` | Disables saving HTTP-requests to HTTP-queue with proxy response in format " *4XX* ", where *XX* – any numbers. The default value is `false` . |
| `StatusCheck` | Setting the delivery status of HTTP-request (displayed in the Management Console), depending on the status code returned by a web or proxy server. If the value is set to true code analysis is performed, which enables a more accurate display of the delivery status for HTTP-request. The default value is `false` |
| `UnsafeMode` | The mode in which, when the error happens, process works stopped and the dump file is being created. The default value is `false` |
| `WCGAuthCache` | Indicates whether authorization data caching feature required for WebSense WSG integration is included. To enable caching set the value to true. The default value is `false` |
| `WCGAuthTTL` | Authorization information caching time if enabled parameter `WCGAuthCache`, in seconds. The default value is `900` |
| `ZimbraMail` | Interceptin Zimbra mail. The default value is `false` |

# The Icq Section

The `Icq` section contains settings for processing copies of ICQ messages, received from Sniffer:

| Parameter | Description |
| --- | --- |
| `DefaultCodepage` | Coding incoming ICQ-traffic. The default value is `cp1251` |
| `DialogBytesCount` | The size of the dialog (in bytes), at which the ICQ-dialog is saved in a file queue. The default value is `500` |
| `DialogTimeout` | Time interval (in minutes), after which the expiration and from the moment of the last interception of ICQ-message you need to save the dialog to the file queue. The default value is `5` |
| `FakeFileTransferPort` | The port, which blocks the attempts to transfer files after redirection to it. The default value is `62225` |

| Parameter | Description |
| --- | --- |
| FormatXmlContext | Formatting XML. Used for debugging. The default value is false |
| MessageWindow | The number of dialogue messages, at which the ICQ-dialog is saved in a file queue. The default value is 10 |
| OCR | Using OCR technology. The default value is false |

## The Smtp Section

The Smtp section contains settings for processing copies of SMTP messages received from Sniffer:

| Parameter | Description |
| --- | --- |
| DumpMode | Adjusts the amount of data that falls into the dump. The default value is false |
| DumpPath | Path to a dump file. The default value is dump.smtp |
| FormatXmlContext | Formatting XML. Used for debugging. The default value is false |
| MaxMsgSize | The size of SMTP-message (in bytes) above which the message is not processed by the System. The default value is 52428800 |
| ReadBufferSize | Amount of data, received from Sniffer at once. The default value is 32768 |

## The oracle.conf configuration file

Parameters of connection with database server:

| Setting | Description |
| --- | --- |
| ConnString | String of connection with database server (server alias from **tnsnames.ora** file) |
| NLS_LANG | Encoding that defines DB localization |
| ORACLE_HOME | Value of ORACLE_HOME environment variable |
| Password | Password of Linux user account |
| Username | Name of Linux user account |

## The cas.conf configuration file

The **cas.conf** configuration file contains the following sections describing settings for content analysis engines:

- The Analysis Section;
- The Thrift Section;
- The Config Section.

## The Analysis Section

The `Analysis` section defines if the analysis engine is enabled (`on` value) or disabled (`off` value).

| Parameter | Description |
|---|---|
| `Autoling` | Automatic linguistic analysis. Default value is `off`. |
| `Classifier` | Content analysis. Parameter contains the following settings:<br>`RelevanceThreshold` – terms threshold. Default value is `0.10000000000000001`;<br>`Spelling` – typos technology. Default value is `off`;<br>`Translit` – transliteration technology. Default value is `off`. |
| `Exclusions` | Exclusions. |
| `FormAnalysis` | Form detector. |
| `Images` | Image detector.<br>Parameter contains the following settings:<br>`Barcode` – barcode-recognition technology. Provides text as an output;<br>`ImageClassifier` – image classificator technology, wich works with passports, drawings, geographical maps;<br>`KeypointMatcher` – technology of searching smaller images on bigger ones. Works on credit cards;<br>`MatcherConfig` – path to the file with the definite analysis settings (image-matcher.yml);<br>`StampDetector` – детектор печатей. |
| `Researcher` | Text objects detector. |
| `Stamper` | Etalon documents detector. |
| `TableAnalysis` | DB ubloadings detector. |

| Parameter | Description |
|---|---|
| | `MinWords` – minimal number of words in a DB unloading file, enough to detect unloading. This number includes all fields names, which contains all table data. It is required, that words are separated from one each other by space or another indented. Default value is `10`. |

## The Thrift Section

| Setting | Description |
|---|---|
| Port | Port on which the Content analysis server receives incoming connections. Default value is 9992 |
| `ServerType` | Server type |
| `TransportType` | Data exchange type. Default type is – socket |

## The Config Section

| Parameter | Description |
|---|---|
| `CacheMaxSize` | Number of content analysis results, which is stored in cash. Number of cash elements. Default value – `10000` |
| `Path` | Path to cas configuration file. Default value – `etc/config/cas` |
| `SchemaPath` | Path to xsd file, which is for xml configuration validity check. Default value – `etc/cas_config.xsd` |

## The expressd.conf configuration file

The **expressd.conf** configuration file is described in the following topics:

- The Expressd Section;
- The Expressd Section, Http Parameter;
- The Expressd Section, Ocr Parameter.

## The Expressd Section

| Parameter | Description |
|---|---|
| `DumpDir` | The directory where to a queue of incoming objects will be saved (the DumpObjects parameter should be enabled). Default value is `/tmp/dump` |
| `DumpObjects` | Enabling (true) or disabling (false) of possibility of saving incoming objects to queue. The default value is `false`.<br>**Note:** it is not recommended to change the value of this setting |

| Parameter | Description |
|---|---|
| `FormatXmlContext` | Enabling (true) or disabling (false) the formatting XML context. Applied for context reading convenience. The default value is `false`. |
| `HTTP` | Configuring HTTP-objects intercepting (see "The Expressd Section, Http Parameter") |
| `ListenAddr` | Address of server network interface where listening process for objects received from InfoWatch Device Monitor and DeviceLock is running. The default value is `0.0.0.0` |
| `ListenPort` | Port of server where listening process is running. The default value is `4101` |
| `MaxBinarySize` | Maximum size (in bytes) of graphical file which will be checked by the System if it corresponds to set fingerprints. Default value is `1048576` |
| `MaxLoadAvg` | Maximum load to the system where process **iw_expressd** (threshold is in terms of nominal units). If the system load equals to specified threshold or exceeds it then process **iw_expressd** stops letters receiving objects. When system load will lower objects receiving will be resumed. The default value is `10` |
| `OCR` | Configuring OCR engine usage (see "The Expressd Section, Ocr Parameter") |
| `TempDir` | Directory for storing temporary files. Default value is `/tmp` |
| `ThreadsNumber` | Maximum number of threads for parallel executing of process **iw_expressd**. The default value is `4`. Increasing number of threads increases the process performance but also increases memory consumption.<br>**Warning!** For correct receiving of objects from InfoWatch Device Monitor please specify the same number of processing threads as is set at the InfoWatch Device Monitor server.<br>Configuring number of processing threads of InfoWatch Device Monitor is specified by parameter `NumberOfConnections` in InfoWatch.DeviceMonitor.Server.exe.config configuration file see details in «*InfoWatchDeviceMonitor. Installation Guide*»). |

# The Expressd Section, Http Parameter

| Setting | Description |
|---|---|
| `CharsetDetection` | Method of text encoding defining. Default value is 0. With this value the encoding is defined as usually. After extracting to the context some POST queries can be displayed incorrectly. To fix this problem you can set `1` value |
| `DecodeHttpContent` | Enabling unpacking of query content if there is Content-Encoding heading with value gzip, deflate or compress. Default value is `true` |

| Setting | Description |
| --- | --- |
| ExtractHttpEntity | Enabling extracting the text from encoded query content by external unpackers. This procedure is implied if there are any failures of internal decoding procedure by zlib. Default value is false |
| MaxMemoryBlock | Maximum size (in kilobytes) of POST query which can be stored in operational memory. Block of bigger sixe will be uploaded to temporary files. Default value is 4096 Kb |
| MinHeader | Minimum text size (in bytes) of one block of variable in URL encoding which will be transferred to the Content analysis server. Default value is 10. |
| MinText | Minimum text size (in bytes) for which the content analysis will be held. Default value is 0 bytes. Configuring of this setting lets lower the load on the Content analysis server. This can be reached by refusing from content analysis of the text which size is as small as does not let to send significant messages. |

## The Expressd Section, Ocr Parameter

| Parameter | Description |
| --- | --- |
| Crawler | Using OCR for files received from Crawler interceptor |
| DM | Using OCR for files received from Device Monitor |
| FTP | Using OCR for files received from FTP Monitor |
| HTTP | Using OCR for files received from HTTP Monitor |
| IMAP4 | Using OCR for received IMAP4 traffic (Mail Monitor) |
| MAPI | Using OCR for received MAPI traffic (Mail Monitor) |
| MMP | Using OCR for files received from MMP Monitor |
| NRPC | Using OCR for files received from Lotus Adapter |
| POP3 | Using OCR for received POP3 traffic (Mail Monitor) |
| Photo | Using OCR for files received from Photo Monitor |
| Print | Using OCR for files received from Print Monitor |
| SMTP | Using OCR for files received from SMTP Monitor |

| Parameter | Description |
| --- | --- |
| `Skype` | Using OCR for files received from Skype Monitor |
| `XMPP` | Using OCR for files received from XMPP Monitor |

## The messed.conf configuration file

| Setting | Description |
| --- | --- |
| HeloDomain | Value of the HELLO command in SMTP dialog. The default value is `smtp.company.com` |
| OCR | Default value is `false` |
| Relay | Full domain name of the mail relay-server that the letter is forwarded to, used for identification within mail protocol. Specified when the System is installing. |
| RelayPort | The port of mail relay-server that the letter is forwarded to. Specified when the System is installing |
| Timeout | Time during which the attempts to deliver SMTP-mails are being made in seconds. After this time, a letter is transmitted to the database. The default value is `1200` |
| WorkerThreads | Maximum number of threads for parallel running of the **iw_messed** process. Default value if `8`. Increasing the number of threads improves process performance but also increases memory consumption |

## The smtpd.conf configuration file

| Setting | Description |
| --- | --- |
| `MaxThreads` | Maximum number of threads for parallel executing of **iw_smtpd** process. Default value is `8`. Increasing number of threads increases the process performance but also increases memory consumption. |
| `MaxMsgSize` | The size of letter (in bytes). Default value is `104857600` |
| `Domain` | Full domain name of the receiving SMTP-server used for identifying within mail protocol. It is recommended to use the name of TM server where **iw_smtpd** process runs. |
| `ListenAddr` | The address of the network interface of the server where listening process runs. Specified when the System is installing. |

| Setting | Description |
| --- | --- |
| `ListenPort` | The port where the server where listening process runs. Specified when the System is installing. |

## The capstack.conf configuration file

The **capstack.conf** configuration file is described in the following chapters:

- UsedProcessors section;
- UsedSources section.

## UsedProcessors section

In `UsedProcesses` section processes are set, which will parse **iw_capstack**. Process parses protocol and converts it into extention . Further the traffic is transmitted to **iw_messed** process (see " Configuration file messed.conf").

| Parameter | Description |
| --- | --- |
| `imap4` | Parsing imap4.Possible values: `true, false`.<br>Default values: true |
| `nrpc` | Parsing nrpc. Possible values: `true, false`.<br>Default values: `false` |
| `pop3` | Parsing pop3. Possible values: `true, false`.<br>Default values: true |

## UsedSources section

In `UsedSources` section parameters of data source are set for **iw_capstack**.

| Parameter | Description |
| --- | --- |
| `iscp` | Using to recieve traffic from component **iw_sniffer**. Default values: `true`.<br>Possible values `true, false` |

## The indexer.conf configuration file

This file contains configuration of indexing module. Indexing parameters are being applied to **iw_indexer** module.In `Indexer` section parameters of working with database and indexing methods are set:

| Parameter | Description |
|---|---|
| ArchiveDir | Path to catalogue to archived indices. Dafault values: sphinx_archive |
| BuildIndexByContent | Extended indexing. Possible values: true, false. Default values: true |
| FetchSize | Number of objects, requested by service from database for further indexing. Dafault value: 4000 |
| IndexExactWords | Exact Match. Possible values: true, false. Default values: false |
| TarPath | Path to backup utility. Default values: /bin/tar |
| WaitTimeInSects | Timeout between attempts to receive objects from DB |

## The web.conf configuration file

The file contains parameters of interaction between Management Console and other System components.

The db section contains parameters of interaction between Management Console and the database:

| Parameter | Default value | Description |
|---|---|---|
| connstring | for Oracle: "localhost/iwtm:pooled",<br>for PostgreSQL: "pgsql:host=localhost;port=5433;<br>dbname=postgres" | String of connection to DB |
| driver | for Oracle: "oci", для PostgreSQL: "pgsql" | Driver type for connecting to DB |
| password | xxXX1234 | Password for DB user |
| schema | iwtm | TM database schema |
| username | iwtm_web | DB user who has permissions to connect and work with tables used by Web-GUI |

The search section contains parameters of interaction between Management Console and the full-text search service:

| Parameter | Default value | Description |
|---|---|---|
| driver | sphinx | Name of the full-text search driver |

| Parameter | Default value | Description |
|---|---|---|
| `hostname` | `localhost` | Server where the search engine is installed |
| `max_matches_common` | `100000` | Maximum number of events that is expected to be found during the full-text search.<br>If the number of results is larger, the **max_matches_maximum** parameter applies.<br>Affects the **average** consumption of memory by **sphinx** service in full-text request |
| `max_matches_maximum` | `10000000` | Maximum number of found events during the full-text search.<br>Affects the **maximum** consumption of memory by **sphinx** service in full-text request |
| `page_size` | `10000` | Number of events received with one request to full-text search (**sphinx** service).<br>Affects the maximum consumption of memory by Web-GUI, including PHP processes |
| `port` | `9306` | Port of MySQL protocol of the **sphinx** service |

## The `kicker` contains services used by Web-GUI:

| Parameter | Default value | Description |
|---|---|---|
| `agent.enabled` | `1` | Is responsible for interaction with the `agent` service: obtaining diagnostic data, restarting services, integrity control. |
| `blackboard.enabled` | `1` | Is responsible for adding/deleting status for persons/computers from policies, adding new contacts to persons during the post-identification, adding new applications to search tooltips for clipboard and screenshots, adding objects from policies to notification queue.<br>Must be enabled to take objects from Blackboard service. |
| `crawler.enabled` | `0` | Must be enabled for interactive operation of **Crawler** section |
| `export.enabled` | `1` | Is responsible for exporting the configuration (classification base, protected objects) |
| `import.enabled` | `1` | Is responsible for importing the configuration (classification base, protected objects) |
| `notifier.enabled` | `1` | Is responsible for sending notifications from the notification queue from policies |
| `report.enabled` | `1` | Is responsible for generating reports in **Dashboard** and **Reports** sections, and for exporting events in the **Events** section |
| `samplecompiler.enabled` | `1` | Is responsible for adding sample documents, blanks, stamps, and database unloadings |

| Parameter | Default value | Description |
|---|---|---|
| `selection.enabled` | `1` | Is responsible for executing requests from **Events** and **Reports** sections |
| `systemcheck.enabled` | `1` | Is responsible for checking notifications from Nagios and interactive updating the Nagios counters in **Administration -> Healthcheck** section |
| `xapisamplecompiler.enabled` | `1` | Is responsible for adding automatic DB unloading and their functioning |

The `serman` section contains parameters of TM server:

| Parameter | Default value | Description |
|---|---|---|
| `hostname` | `localhost` | Server where `serman` is installed |
| `port` | `9998` | Number of port with `serman` |
| `username` | `serman_client` | Name of `serman` user |
| `password` | `xxXX1234` | Password for `serman` user |

Other parameters:

| Parameter | Default value | Description |
|---|---|---|
| `mail.line_break` | `0` | When enabled, the "\r\n" delimiter is replaced with "\n" in notification emails. Applies when notification are received from policies of incorrect type |
| `version` | `Current version` | Current version of the product |
| `debug` | `0` | Switching to debug mode |
| `slowRequestTime` | `0` | Saving dump only for HTTP requests that are larger than the specified seconds or erroneous HTTP requests |
| `rotateDebug` | `true` | Enabling debug JSON rotation |
| | `false` | Enables the insertion of text to JSON files instead of writing it to a separate file when saving debug information on the event |

| Parameter | Default value | Description |
|---|---|---|
| `inlineTextDump` | | |
| `maxInlineDumpSize` | `1048576` | Maximum length of a piece of text to be inserted to JSON.<br>If the length exceeds the specified value, a separate file is created |

## The analysis.conf configuration file

File contains auxiliary data to **iw_analysis** module . **analysis.conf** configuration file contains the following sections:

- The Analysis section;
- The Bookworm section.

## The Analysis section

| Parameter | Description |
|---|---|
| `CharsetDetection` | Method of text encoding defining. Default value is 0. With this value the encoding is defined as usually. After extracting to the context some POST queries can be displayed incorrectly. To fix this problem you can set `1` value |
| `DecodeHttpContent` | Enabling unpacking of query content if there is Content-Encoding heading with value gzip, deflate or compress. Default value is `true` |
| `ExtractHttpEntity` | Enabling extracting the text from encoded query content by external unpackers. This procedure is implied if there are any failures of internal decoding procedure by zlib. Default value is `false` |
| `MaxMemoryBlock` | Maximum size (in kilobytes) of POST query which can be stored in operational memory. Block of bigger sixe will be uploaded to temporary files. Default value is `4096` Kb |
| `MaxReadBuf` | Buffer size limitation. Default value is 131072 |
| `MinHeader` | Minimum text size (in bytes) of one block of variable in URL encoding which will be transferred to the Content analysis server. Default value is `10` |
| `MinText` | Minimum text size (in bytes) for which the content analysis will be held. Default value is 0 bytes. Configuring of this setting lets lower the load on the Content analysis server. This can be reached by refusing from content analysis of the text which size is as small as does not let to send significant messages |
| `OnlyPost` | Only POST-requests interception. Default value is `true` |

| Parameter | Description |
|---|---|
| ZimbraMail | Zimbra mail interception. Default value is false |
| OCR | Configuring OCR engine usage. Default value is false |
| TempDir | Directory for storing temporary files. Default value is tmp |
| WorkThreads | Maximum number of threads for parallel executing. Default value is 12 |

## The Bookworm section

| Parameter | Description |
|---|---|
| ConnectTryCount | Number of connection attempts. Default value is 5 |
| CacheDuration | Time of **iw_bookworm** reference data validity. Default value is 15 |

## The sample_compiler.conf configuration file

| Section/Parameter | Description |
|---|---|
| Bookworm | Section defines **iw_bookworm** parameters |
| EnableOCR | Enable using OCR. Default value is false |
| Logging | see article "The Logging Section" |
| NookDir | see article "The Nookdir Section" |
| OutChunckSizeLimit | Maximum size of the chuck, to which compilation resultes are returned. Default value is 1048576 |
| ResourceLimits | Limitation of system resources used by the program |
| Stratup | see article "The Startup Section" |
| Technologies | Section of individual technologies configuration |
| ThreadsCount | The number of processing threads. Default value is 5 |

| | |
|---|---|
| `ThriftServers` | Parameters of thrift-server, which is used by **sample_compiler** to recieve tasks for data compilation |

## The loader.conf configuration file

| Section | Description |
|---|---|
| OracleUtf8Processing | Indexing text with unprintable characters. Includes the following parameters:<br>• `Enabled`. Default value is `true`.<br>**Note:**<br>In case indexing unprintaple characters is not required, speed up System work by changing value to `false`.<br>• `Substituter`. Default value is `95`. (Instead of unprintable symbol several undercores will be inserted depenfing on the byte lenght of utf-8 symbol. Any utf-8, which is longer, than 3 bite is replaced by undercore symbols.)<br>If unprintable symbol is 1 byte and any value of `Substituter` which is less or equals `127`, a ddditional tokens will be fractioned when indexing.<br>This might be useful in individual cases (for example, [`word1/smile/word2`] - for correct indexing `word1, word2`).<br>**Warning!**<br>It is not recommended to use values from service ascii. This might cause indexing problems. |

## The configerator.conf configuration file

| Parameter | Description |
|---|---|
| `Debug` | Enable/disable detailed logging. Default value is `false`. It is not recommended to edit parameter without InfoWatch employee's control |
| `ConfigurationsCount` | Number of configurations, saved in `etc/configerator/` catalogue. (Value can be increased in case connections are too slow and configurations are not transmitted to DM. To save storage, one must decrease value). Default value is `100`. |
| `WebSocketURL` | URL, which is used to send notifications, that configuration has been updated. It is recommended to change parameter in case nginx has been configured unconventionally. Default value is `https://localhost/api/notify/publish/configUpdate` |

# 7.3 Configuring Settings for HTTP-Requests Transferred through ICAP Protocol (icap.conf file)

> **Note:**
>
> The **icap.conf** file is created only after installation of ICAP integration module.

The **/opt/iw/tm5/etc/icap.conf** file defines settings of interaction with ICAP server:

| Setting | Description |
|---|---|
| `AllMethods` | Enables anlysis of all http traffic. Default value is `false`. Only `PUT`-requests are processed. |
| `AsyncCheck` | Traffic transmission happens before its analysis. Default value is `false`. |
| `DisableIPv6` | Disabling (`disable_ipv6 = true`) or enabling (`disable_ipv6 = false`) supporting connections by IPv6 protocol. By default the supporting is disabled.<br>If IPv6 supporting is disabled at ICAP server then **iw_icap** service will be running only if the option is enabled, i.e. `disable_ipv6 = true`. |
| `ErrorHTML` | Path to HTML file containing message which web-browser outputs if the System blocks user's request. Default value is `etc/error.html`. (path regarding current catalogue – root System catalogue) |
| `ForceKeepAlive` | Using one TCP -connection to send or get multiple HTTP -requests and responses instead of opening a new connection for each request - response pair |
| `ListenPort` | Port where ICAP server listens HTTP requests from proxy server with ICAP client. Ports with numbers greater than 1025 are acceptable. Default value is `1344` |
| `LogBlock` | Setting for log level not less than 4 (LogLevel=4). Defines if messages about blocking of intercepted HTTP requests are logged to the system log. Default value is `0`: not logged |
| `LogTimer` | Defines if the time of HTTP requests' processing is logged to the system log. `1` – the time is logged. Default value is `0` – not logged |
| `MaxConnections` | Maximum number of connections. Default value is `100`. |
| | Maximum file size in kilobytes to be held in memory: `4096` |

| | |
|---|---|
| `MaxMemoryBlock` | |
| `MinDataLength` | Minimum volume (in bytes) of URL variable which will be transferred to the Content analysis server. Default value is `10`. |
| `MinTextLength` | Minimum text size (in bytes) for which the content analysis will be held. Default value is 5 bytes. Configuring of this setting lets lower the load on the Content analysis server. This can be reached by refusing from content analysis of the text which size is as small as does not let to send significant messages. |
| `PathTemporary` | Path to storage of ICAP server's temporary files (`/opt/iw/tm5/tmp/icap` by default) |
| `SessionTimeout` | Time, after which session gets disconnected. Default value is `330` |
| `ZimbraMail` | Parameter for working with Zimbra mail server. Default value is `false` |

# 7.4 Configuring Settings of Enclosures Archives Processing

One can configure processing of enclosures in two different configuration files: **/opt/iw/tm5/etc/ config-perm/bookworm/extractors.xml** and **/opt/iw/tm5/etc/extractors.conf**.

In this chapter:

- The extractors.conf Configuration File;
- The extractors.xml Configuration File.

## 7.4.1 The extractors.conf Configuration File

The **/opt/iw/tm5/etc/extractors.conf** contains local settings for extractors.

| Parameter | Description |
|---|---|
| `Dreamcatcher` | Directory in which files which failed to be unpacked are stored |
| `MaxRecursiveLevel` | Maximum nesting level. Default value is `100` |

| | |
|---|---|
| TempDir | The temporary directory for unpacking results. Default value is tmp |

## 7.4.2 The extractors.xml Configuration File

The **/opt/iw/tm5/etc/ config-perm/bookworm/extractors.xml** file contains directory settings and signatures base which define file types when unpacking archives and enclosures.

| Parameter | Description |
|---|---|
| FilenameCharsets | If file name encoding differs from the standard one (ANSI, UTF) then the filename processes as corresponding to encodings listed in this setting. Several values are listed comma separated; the System sequentially tries process the filename in listed encodings while it finds a matched one. Default value is UTF-8,cp1251,cp866 |
| MinFileSizeInBytes | Minimum file size (in bytes) subjected to unpacking. This limit lets increase the System performance due to refusing of small files unpacking. Default value is 10 |
| MaxTextPlainSizeInKb | Maximum size of file, which signature is not defined . Exceeding the threshold value file is automatically considered to be binary and is not sent to **iw_cas**. Default value is 25600 |
| SpeedInKBs | Proposed extractor's operation speed, in Kb/s, per 1 GHz of the processor. Default value is 100 |
| TimeoutInSec | Awaiting time (in seconds) till file processing ends. Default value is 1800 |
| UseLog | Logging extractor. Default value is false |

If the general values of TimeoutInSec and MinFileSizeInBytes settings are not appropriated for some file types then enable these parameters in sections of needed file types with other values.

Other sections define signatures used for detection of types of files from archives and enclosures. Each section contains the same set of parameters:

| Parameter | Description |
|---|---|
| Extension | Extension of archive files. Optional parameter which is needed for correct operation of some archiving utilities requiring correct extensions of incoming files<br>**Example**:<br>Ext = arj |
| Name | Format name. Used for exact detection of format name when file unpacking.<br>To define detection/detailing of format the setting can include a list of names: |

| Parameter | Description |
| --- | --- |
| | "defaultname, name1(code1), name2(code2)"<br><br>In this case the format can be defined basing on the code (codeN) assigned to the file when unpacking. For example if the unpacking is ended with code1 code that the file is considered as having name1 format. The list of names can include default name (defaultname) which will be assigned when the code is not assigned:<br><br>**Example 1 (one format name)**<br><br>text/xml<br><br>**Example 2 (list of format names)**<br><br>"application/arj, UNKNOWN(9), text/encrypted(4)"<br><br>the file format is defined as application/arj. Two others for specific cases are: unknown format (UNKNOWN), encrypted format (text/encrypted) |
| Signature | Format signature which is «standard» sequence of values (bytes) with initial displacement and masks. This sequence is needed for unambiguous definition of files format by the content of those files.<br><br>The signature can include up to 16 triades of the following view:<br><br>[OFFSET]:BYTE_VALUE/[MASK]<br><br>There can be string signature like "BZh" for BZIP2. This signature means specified bytes sequence from 0 displacement. The search of string signatures is performed except for upper/lowercase distinction.<br><br>The OFFSET setting is optional. By default it equals 0 for the first byte and increases by 1 for each later one. The displacement can be specified using «?» symbol – searching of the pattern in first N bytes of a file. For example to search pattern in first 500 bytes you should specify '500?' displacement.<br><br>The MASK setting is optional and equals to 0xFF by default.<br><br>**Example** (signature of a heading of WAV format):<br><br>Sign = "'RIFF', 0x8: 'WAVEfmt'"<br><br>Starting from 0 displacement there is a sequence 'R', 'I', 'F', 'F', then from 8 displacement there should be 'W', 'A', 'V', 'E', 'f', 'm', 't' |
| Comment | The explanation commentary, for example, indicating the version of archiving utility:<br><br>Comment = "bzip2 v. 1.0.x" |
| Command | Command string for file extracting, for example,<br><br>Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}"<br><br>where ${OUTDIR} is a catalogue where to the archive will be extracted and ${SRC} is a name of file to unpack |
| ExcludeFromContext | If the parameter is enabled (On) then the file is unpacked but information on archiving utility is not added to object's XML-context. This lets to let out the fictional containers like MS-TNEF from object's context. By default the parameter is disabled (Off) |
| CaseInsensitive | Indicates whether the symbol register will be taken into account in file processing or not. Default value is false |

| Parameter | Description |
| --- | --- |
| `CreateTags` | Indicates if there is an extracting of the metadata from the file when proceeding by TM extractors. |
| `Archive` | Regulates the kind of retrieved information. When `true` - files. When `false` - data. |

# 7.5 Archiving a Mail Queue Directory

If errors occur in the incoming SMTP mail queue, you must archive the SMTP mail queue folder and save it for further analysis. Then delete the folder. The location of the mail queue folder is specified in **/opt/iw/tm5/etc/filequeues.conf** configuration file in the `Smtppath` section.

# 7.6 Logging System work

To monitor processes, logging subsystem has 6 levels of logging:

| Value | Description |
| --- | --- |
| `fatal` | Writes errors, which stops further process functioning |
| `error` | Writes messages about errors, which are not critical for process functioning |
| `warning` | Writes information about potentially dangerous situations |
| `Information` | General useful information about the process (start/stop, applying configuration and so on) |
| `debug` | Writes information, which is mostly used for service functioning diagnostics (IT, system administrators and so on) |
| `trace` | Mostly used by programmers to track code |

### Configuring logging levels

> **Warning!**
>
> Keep in mind that an increase in the logging level may dramatically reduce System performance.

Configuration files are located in directory `/opt/iw/tm5/etc`. All processes have warning logging level by default `warning`.

**To change logging level for Traffic Monitor Server processes:**

1. In configuration file of required process, in section `Logging` set for parameter `GlobalLevel` required value.
2. Save changes.
3. After committing changes to system journal, restart process:
   `service iwtm restart service_name`

All processes logs are being saved in catalogue `/var/log/infowatch`.

For extractors, which do not have an individual configuration file, logging level can be set in configuration file **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml**:

1. Open configuration file;
2. For parameter `text-extractor` add value `-l <level>`
3. Where <level> is the recording level.
   Example:
   },
   "docx": {
   "Command": [
   "bin/text-extractor –l error -t ooxml -i
   Dollars {{SRC} -d $ {OUTDIR}"
4. After committing changes, restart processes:
   `service iwtm restart bookworm`
   `service iwtm restart warpd`

> **Note:**
>
> This logging configuration is only available for extractors of the following formats: docx, html, msoffice_xml, msole, odp, odt, pptx, xlsx, xml

# 7.7 File queues

**To enable loading the existing object queues:**

1. Stop the following services: icap, smtpd, expressd, sniffer, xapi_xapi, xapi_puppy, analysis, messed, proxy_http, proxy_icq, proxy_smtp, capstack.
2. Place objects from the queue of errors to the required queue.
3. Wait until all objects in the file queue are processed.
4. Start the following services: icap, smtpd, expressd, sniffer, xapi_xapi, xapi_puppy, analysis, messed, proxy_http, proxy_icq, proxy_smtp, capstack.

To start all services, enter the command: **service iwtm start**.

Commands for starting/stopping separate services:

| Starting | Stopping |
|---|---|
| service iwtm start icap | service iwtm stop icap |
| service iwtm start smtpd | service iwtm stop smtpd |
| service iwtm start expressd | service iwtm stop expressd |
| service iwtm start sniffer | service iwtm stop sniffer |
| service iwtm start xapi_xapi | service iwtm stop xapi_xapi |
| service iwtm start xapi_puppy | service iwtm stop xapi_puppy |
| service iwtm start analysis | service iwtm stop analysis |
| service iwtm start messed | service iwtm stop messed |
| service iwtm start proxy_http | service iwtm stop proxy_http |
| service iwtm start proxy_icq | service iwtm stop proxy_icq |
| service iwtm start proxy_smtp | service iwtm stop proxy_smtp |
| service iwtm start capstack | service iwtm stop capstack |

> **Note:**
>
> When the process is complete, make sure that the services are running.

Traffic Monitor has the following queues:

| Path to the directory of the queue | File format in the queue |
|---|---|
| `queue/blackboard` | `.dat` |
| `queue/blackboard_errors` | `.dat` |
| `queue/whiteboard` | `.dat` |
| `queue/errors` | `.xml & .dat` |
| `queue/xml2liro-errors` | `.xml & .dat` |
| `queue/db` | `.xml & .dat` |
| `queue/smtp` | `.xml & .dat` |

Each queue contains additional technical queues which allow you to monitor for processing objects:

- - `.db`
  - `.out`
  - `.in`

Example:
`queue/db/.out`

`queue/db/.in`

`queue/db/.db`

For SMTP queue, the processing is divided into the following stages:

1. `queue/smtp/.in` the file is formed in the given queue as objects are received from Postfix by module `smtpd`. If for some reason an object is delayed in the queue, you must check modules `smtpd` or `proxy_smtp`.
2. `queue/smtp/.db` upon completion of processing the file is moved from the queue `.in` to the queue `.db`.
3. `queue/smtp/.out` - the object is moved to this queue by the next module in the chain (for queue `smtp` - by module `messed`).

Objects are placed in a queue by means of the following modules:

- INPUT – a module which places events to the queue.
- OUTPUT – a module which takes events from the queue.

| Queue name | INPUT | OUTPUT |
|---|---|---|
| queue/smtp | smtpd and proxy_smtp | messed |
| queue/db | messed, icap, expressd, proxy_icq, proxy_http | xml2liro |
| queue/errors | all components if an error occurred during processing | no |
| queue/xml2liro_loader | xml2liro | loader |
| queue/blackboard | luaengined | blackboard |
| queue/blackboard_errors | an error when processing blackboard | no |
| queue/whiteboard | luaengined | whiteboard |
| queue/rails_connector_errors | an error when inserting data loader | no |
| queue/xml2liro-errors | Processing errors xml2liro | no |

# 7.8 Recovering the System after Failures

You can recover the System when server failures occur or during a network outage by completing the steps described below:

1. Stop the processes of the Traffic Monitor Server by running the command:
   service iwtm stop
2. Move all objects from the queues where errors occur to the normal ones. To perform the procedure use iw_qtool utility (see knowledge base article "Moving of Objects between Queues (iw_qtool Utility)").
3. When these operations are completed, check the connection to the Oracle DBMS by running the command:
   `sqlplus db_login/db_password@tns_name`
   here `db_login` and `db_password` are the name and password of database scheme owner, and `tns_name` is the name of TNS service.
   If the test is successful, the following SQL *Plus prompt will be displayed in response to the command:
   `SQL>`
4. Run the Traffic Monitor Server processes by executing the commands:
   `service iwtm start`

After the Traffic Monitor Server is started, check the system log for errors. The path to the system log:

`/var/log/messages`

If the system log contains any error messages, consult technical support service.

# 7.9 Managing morphology languages

Managing morphology languages in Traffic Monitor is being performed through configuration file change and installation of package with language dictionary.

English morphology dictionary is being installed in the System by default.

To add Russian morphology dictionary to preinstalled dictionaries, select `Russian` value in **CFDb** parameter on step of localization parameters selection in the process of System installation (Find information on installation in document "InfoWatch Traffic Monitor 6.0. Installation guide").

Upon installation, user also can:

- Add new morphology language ;
- Update installed morphology language;
- Delete morphology language.

### 7.9.1 Adding new morphology language

Configuration of morphology and Categories and terms languages is being performed in `sphinx_languages` parameter of **sphinx_options.ini** configuration file.

**To add new dictionary to the System**:

1. Stop the **searchd** process:
   `service searchd stop`
2. Stop the **iw_indexer** process:
   `service iwtm stop indexer`
3. Open **sphinx_options.ini** file:
   `vim /opt/iw/tm5/etc/sphinx_options.ini`
4. Add `'morphology language'` value for `sphinx_languages` parameter .
   For example, adding new german dictionary, configuration file will look as follows:
   `sphinx_languages = 'rus deu'`
5. Go to the dictionary packages directory:
   `cd opt/disrt/infowatch/traffic-monitor/Linux`
6. Run the installation packages:
   rpm -i name_of_a_package
   `For example:`
   rpm -i iwtm-sphinx_dict-deu-6.x-yz.x86_64.rpm
7. Run the **iw_indexer** process:
   `service iwtm start indexer`

> **Note:**
>
> To set language priority, make language parameter the last in the list of `sphinx_languages` parameters of **sphinx_options.ini** file.

> **Note:**
>
> Installing new dictionary full database reindexing happens.

### 7.9.2 Updating installed morphology language

**To update existing dictionary**:

1. Go to directory with dictionary packages:
   `cd opt/disrt/infowatch/traffic-monitor/Linux`

2. Run package installation:
   `rpm -i название пакета`
   For example:
   `rpm -i iwtm-sphinx_dict-deu-6.x-yz.x86_64.rpm`

> **Note:**
>
> Updating dictionary, database reindexing will not take place. Language support will be performed only for new events.

### 7.9.3 Deleting morphology language

Configuration of morphology and CFDB languages is being performed in `cfdb_language` parameter of **database.conf** configuration file.

**To delete dictionary from the System:**

1. Stop the **searchd** process:
   `service searchd stop`
2. Stop the **iw_indexer** process:
   `service iwtm stop indexer`
3. Open the **database.conf** file:
   - `vim /opt/iw/tm5/csw/oracle/database.conf` when using Oracle database.
   - `vim /opt/iw/tm5/csw/postgresql/database.conf` when using Postgre SQL.
4. Delete the `'morphology language'` value from the `define cfdb_language` parameter.
5. Remove indexing files from directory:
   `/var/lib/sphinx/`
6. Run the **iw_indexer** process.
   `service iwtm start indexer`

> **Note:**
>
> After dictionary removal full database reindexing takes place.

As a result of morphology language deletion, CFDB language will be deleted from the System as well.

To keep CFDB language, add `'morphology language'` value to `cfdb_language` parameter of **database.conf** configuration file immediately before updating the System. Wherein morphology language will be as well restored.

To remove morphology language after System update, once again delete 'morphology language' value from `cfdb_language` parameter of **database.conf** configuration file .

# 7.10 Configuring serman.conf when changing DB Server Address

In the case of DB sever IP-address change, define new DB server IP-address in `DefaultInterface` parameter of `Serman` section in **serman.conf** configuration file.

# 7.11 Configuring Forwarding Data to SIEM

Integration of Traffic Monitor with SIEM systems (ArcSight, Tivoli) is being performed through built-in features of the program. Configuring this functionality is possible using **setup** utility, which is available on Traffic Monitor server.

Integration means forwarding consolidated information installed TM components to SIEM.

**Information from TM is available for SIEM system:**

1. By means of a table view:
   - Events, registered in TM;
   - TM Console user session audit;
2. By means of rsyslog:
   - Logging in and out TM Linux server;
   - Events, registered in TM Linux server system journal, including information on logging in and out Oracle or Postgre DB users;
   - State of TM services on Linux server or group of servers.

In this chapter:

- Configuring SIEM side;
- Configuring TM side;
- Type of logs, transmitted to SIEM.

## 7.11.1 Configuring SIEM side

**To prepare SIEM to recieving data from TM**:

1. In SIEM tables to extract information from:
   - `IWTM.ARC_VIEW_OBJECTS`
     TM events
   - `IWTM.ARC_VIEW_AUDIT_LOG`
     TM user audit
2. Create SIEM account to access DB tables.
3. Configure processing data, which has been extracted from TM DB.

To analyse table views of TM events and user audit see articles "TM events table view" and "User audit table view".

> **Warning!**
>
> While configuring integration, additional modules from SIEM system vendor, which allow SIEM system to work with table views, can be required. For example, HP Flex Conector module is required for integration with HP ArcSight.

## TM events table view

Connect to TM DB using created siem user (see "Creating siem user"). IWTM. ARC_VIEW_AUDIT_LOG contains desired data.

| Attribute name | Data type | Description | Possible values | Example |
|---|---|---|---|---|
| object_id | Number (20) | Event ID attribute. | TM BD event ID. Always present. | 110 |
| monitorcode | Varchar2 (4000) | Event type attribute. | Possible values:<br>• Email<br>• ICQ,<br>• GTalk,<br>• Ya.online,<br>• Mail.Ru Agent,<br>• Skype,<br>• MSN,<br>• SMS,<br>• Jabber,<br>• Web message,<br>• File exchange,<br>• Copying to an external device,<br>• Print,<br>• Crawler (storing data on workstations, Share Point, network resources),<br>• MS Lync,<br>• Photo (photo on a mobile device), | Crawler |

| Attribute name | Data type | Description | Possible values | Example |
|---|---|---|---|---|
| protocol | | Event attribute Protocol. | Possible value:<br>• OSCAR.<br>• Skype;<br>• XMPP;<br>• MMP;<br>• SIP;<br>• YMSG;<br>• WhatsApp<br>• FTP;<br>• POP3;<br>• IMAP;<br>• MAPI;<br>• SMTP;<br>• HTTP;<br>• HTTPS;<br>• NRPC;<br>• None. | |
| verdict | varchar2 (12) | Verdict. | Possible values:<br>• Quarantined,<br>• Forbidden,<br>• Allowed. | Forbidden |
| date_of_capture | Varchar2 (50) | Date of capture attribute in UTC and date of capture timezone. | | 2014-06-19T18:56:26+04:00 |
| device | varchar2 (256) | Device name attribute. | Name of device, on which information has been copied.<br>Or name of the printer, to which copy of intercepted document has been sent.<br>Can be empty. | Kingston USB Drive 5.0 |

| Attribute name | Data type | Description | Possible values | Example |
|---|---|---|---|---|
| Web-source | varchar2 (256) | Resource attribute. | Address of visited web-source or cloud storage address.<br>Can be empty. | Yahoo.com |
| recipientscontacts | clob | Recipients attribute. | List of recipients, separated by commas, in <contact type>:<contact value> format.<br>The following contact exists:<br>- auth<br>- email<br>- icq<br>- skype<br>- mobile<br>- phone<br>- sid<br>- webaccount<br>- lotus<br>Can be empty. | email: ivanov@infowatch.ru, email:petr. petrov@infowatch.ru |
| recipientsfullname | clob | Recipients attribute. | List of recipients' full names, separated by commas.<br>Specified only in case recipient has been identified.<br>Can be empty. | Ivanov Ivan Ivanovich,<br>Petrov Petr Petrovich |
| recipientsdomainaccountname | clob | Recipients attribute. | List of authenication keys (like "auth") for all recipients, separated by commas.<br>Can be empty. | Ivanov@iw,<br>Petrov@iw |
| senderdomainaccountname | clob | Sender attribute. | Authenication of "auth" type.<br>Can be empty. | Petrov@iw |
| senderfullname | clob | Sender attribute. | Sender's full name.<br>Can be empty. | Petrov Petr Petrovich |
| sendercontact | clob | Sender attribute. | Sender's contact in <contact type>:<contact value> format. | email:petr. petrov@infowatch.ru |

| Attribute name | Data type | Description | Possible values | Example |
|---|---|---|---|---|
| | | | The following contact exists:<br>- auth<br>- email<br>- icq<br>- skype<br>- mobile<br>- phone<br>- sid<br>- webaccount<br>- lotus<br>Can be empty. | |
| sendermachinedomainname | clob | Workstation attribute. | Domain name of sender's workstation.<br>Can be empty. | XP-PETROV |
| sendermachineip | clob | Workstation attribute. | IP-address of sender's workstation.<br>Can be empty. | 10.60.20.184 |
| perimetersin | clob | Name of perimeter, which event has entered. | List of perimeters' names, which event has entered, separated by commas.<br>Can be empty. | Company perimeter |
| perimetersout | clob | Name of perimeter, which event has left. | List of perimeters' names, which event has left, separated by commas.<br>Can be empty. | Company perimeter |
| tags | clob | Tag attribute. | List of tags, separated by commas.<br>Can be empty. | New |
| categories | clob | Category attribute. | List of attributes, separated by commas.<br>Can be empty. | Confidentially |
| text_objects | clob | Text object attribute. | List of text objects, detected in intercepted object, separated by commas.<br>Can be empty. | special control |

| Attribute name | Data type | Description | Possible values | Example |
|---|---|---|---|---|
| fingerprint | clob | Sample form, sample document, sample stamp, sample tables attribute. | List of sample forms, sample documents, sample stamps, sample tables, detected in intercepted object, separated by commas.<br>Can be empty. | Application form.doc |
| protecteddocument | clob | Event attribute. Protection object. | List of protection objects, discovered in intercepted object, separated by commas.<br>Can be empty. | Lease contract |
| policy | clob | Policy attribute. | List of policies, which triggered on intercepted object, separated by commas.<br>Can be empty. | New employees monitoring policy |
| protecteddocument | clob | Event attribute Protection object. | List of policies name, triggered on the intercepted object, separated by commas.<br>Can be empty. | Lease contract |
| policy | clob | Event attribute. Policy. | List of policies name, triggered on the intercepted object, separated by commas.<br>Can be empty. | Control policy for new employees |
| violationtype | varchar2 (40) | Violation type attribute. | Possible values:<br>- Copy<br>- Placement<br>- Transfer<br>Can be empty. | Copy |
| userdecision | varchar2 (27) | User decision attribute. | DLP console user decision.<br>Possible values:<br>- Violation,<br>- NoViolation,<br>- NotProcessed,<br>- AdditionalProcessingNeeded.<br>Can be empty. | Violation |

| Attribute name | Data type | Description | Possible values | Example |
|---|---|---|---|---|
| filepath | clob | File path attribute. | List of file paths', separated by commas.<br>Can be empty. | \\xp-petrov\C$\666.txt |
| attachments | clob | Event attribute. Name of the attachment file. | Names of attachment files, separated by commas. | 666.txt, Petrov.doc, 3.jpg |
| url | varchar2 (4000) | URL attribute. | Full address, from which data transmission has been performed.<br>Can be empty. | 10.60.21.34/3.jpg |
| capture_server_ip | varchar2 (256) | Interception server IP attribute. | IP server, on which data has been intercepted.<br>Can be empty. | 10.60.21.34 |
| capture_server_hostname | varchar2 (256) | Name of interception server attribute. | Name of server, on which data has been intercepted.<br>Can be empty. | iwtm.infowatch.ru |

## User audit table view

Connect to TM DB using created **siem** user (see "Creating siem user"). IWTM.ARC_VIEW_AUDIT_LOG contains desired data.

| Attribute | Data type | Desctiption | Example |
|---|---|---|---|
| audit_log_id | Number (20) | TM user session audit entry ID. | 12345 |
| change_date | Varchar2 (50) | Date and time of registered user action | 2014-06-19T18:56:26+04:00 |
| user_login | varchar2 (256) | Login of user, who performed an action | Admin |
| user_fullname | varchar2 (256) | Full name of user, who performed an action | Petrov Petr Petrovich |
| user_email | varchar2 (256) | Email of user, who performed an action | petr.petrov@infowatch.ru |
| operation | | Type of action, performed by user | Edit |

| Attribute | Data type | Desctiption | Example |
| --- | --- | --- | --- |
| | varchar2<br>(40) | The following values are possible:[VK1]<br>• Run (performing query)<br>• Start (start)<br>• Stop (stop)<br>• view (view)<br>• create (creation)<br>• update (editing)<br>• delete (delition)<br>• login_failure (unsuccessful login attempt)<br>• login (successful login)<br>• logout (logout)<br>• change_password (password change)<br>• decision_update (changin user decision)<br>• remove_tag (changing event tag)<br>• delete_ref (deleting reference)<br>• copy (copying)<br>• move (move)<br>• commit (applying changes in system configuration)<br>• rollback (cancellation of changes in system configuration)<br>• draft (saving changes in system configuration)<br>• add (adding)<br>• import (import)<br>• export (export) | |
| `entity_type` | varchar2<br>(40) | Type of object on which the action was carried out.<br>The following values are possible:[VK2]<br>• Category (category)<br>• Dashboard (dashboard)<br>• DashboardWidget (widget)<br>• EtForm (sample form) | Dashboard |

| Attribute | Data type | Desctiption | Example |
|---|---|---|---|
| | | • EtStamp (sample stamp)<br>• EtTable (sample table)<br>• Fingerprint (sample documents)<br>• LdapContact (LDAP contact)<br>• LdapGroup (LDAP group)<br>• LdapPerson (LDAP person)<br>• LdapStatus (LDAP person status)<br>• LdapWorkstation (LDAP workstation)<br>• Perimeter (perimeter)<br>• Policy (policy)<br>• Report (report)<br>• Role (role)<br>• Selection (selection)<br>• SystemList (list of resource topics)<br>• SystemListItem (list of resources with definite topic)<br>• Tag (tag)<br>• Term (term)<br>• TextObject (text pbject)<br>• User (пользователь)<br>• VisibilityArea (visibility scope)<br>• Config (configuration)<br>• License (license)<br>• Object (object)<br>• ProtectedCatalog (protected catalog) | |
| `entity_display_name` | varchar2 (4000) | Name of object, on which the action was carried out. | Statistics1 |
| `property_changes` | clob | Description of actions in json format. Filled only in case of managing users, roles, areas and logging in and out of the management console.<br>Three different formats are possible. | |
| | | **Format №1.** | |

| Attribute | Data type | Desctiption | Example |
|---|---|---|---|
| | | Relevant for events of role and visibility scope management. | |
| | | {<br>“old”: {<br>“<OBJECT TYPE>”:{<br>{<br>“<FIELD>”: “<VALUE>”,<br>“<FIELD>”: “<VALUE>”<br>}<br>}<br>}<br>{<br>“new”: {<br>“<OBJECT TYPE>”:{<br>{<br>“<FIELD>”: “<VALUE>”,<br>“<FIELD>”: “<VALUE>”<br>}<br>}<br>}<br>} | {<br>"old":{<br>"visibilityareas":{<br>}<br>},<br>"new":{<br>"visibilityareas":[<br>{<br>"VISIBILITY_AREA_ID":"<br>F00207A1E7E7743EE0433D003C0A5DD400000000",<br>"DISPLAY_NAME":"<idclip>",<br>"NOTE":"<idclip>",<br>"VISIBILITY_AREA_CONDITION":"{"data":{"link_operator":"<br>and","children":[]}}",<br>"IS_SYSTEM":1<br>}<br>}<br>} |
| | | **Format №2.**<br>Relevant for user management events. | |
| | | {<br>“old”:{<br>“<FIELD>”: “<VALUE>”,<br>“<FIELD>”: “<VALUE>”<br>}<br>“new”:{<br>“<FIELD>”: “<VALUE>”,<br>“<FIELD>”: “<VALUE>” | {<br>"old":{<br>"EMAIL":"asdasd@asdasd.ru",<br>"CHANGE_DATE":"01-07-2014 09:46:29.000000"<br>},<br>"new":{<br>"EMAIL":"asdasd11@asdasd.ru",<br>"CHANGE_DATE":"01-07-2014 09:46:44.000000" |

| Attribute | Data type | Desctiption | Example |
|---|---|---|---|
| | | }<br><br>} | }<br><br>} |
| | | **Format №3.**<br><br>Relevant for log in and log out events. | |
| | | {<br><br>"request":{<br><br>"hostname": “<HOST NAME>”,<br><br>"ip":"<IP-ADDRESS>",<br><br>"login":"<USER LOGIN>"<br><br>}<br><br>} | {<br><br>"request":{<br><br>"hostname":null,<br><br>"ip":"127.0.0.1",<br><br>"login":"officer"<br><br>}<br><br>} |

## 7.11.2 Configuring TM side

**To configure forwarding consolidated information to TM**:

1. Start **setup** utility menu.
2. Create DB user account for SIEM (see "Creating siem user").
3. Configure forwarding information from TM to SIEM (see "Forwarding logs to SIEM");
4. Configure **Nagios** and TM components from menu;
5. Configure TM DB user session audit logging.

## Forwarding logs to SIEM

**To configure forwarding entries from Linux-server log files to SIEM**:

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose **iwtm-siem** option.
4. Choose **Log messages forwarding configuration** option.
5. Set parameters for logs transfer:

| Parameter | Description |
|---|---|
| `Enable forwarding` | Enabling/disabling forwarding logs to siem. (Possible value: `Yes`/`No`) |

| | |
|---|---|
| `Forwarding server` | SIEM IP-address or dns-name |
| `Forwarding server port` | Port of SIEM server, where **syslog** is running |
| `Forwarding protocol` | Protocol of forwarding data to SIEM. (Possible value: `TCP/UDP`) |
| `Log messages severity` | Minimal level of log-messages, sent to SIEM server. (Possible value: `Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug`) |
| `Size (MB)` | Acceptable size of message queue |

6. Press **Ok**.

> **Warning!**
>
> Disconnecting users with administrative permissions is not being logged in DB, thereafter, this information will not be forwarded to SIEM.

## Managing TM DB user sessions

Enabling and disabling TM DB user sessions logging to OS system journal is being performed via **rsyslog** utility.

**To enable TM DB user sessions logging**:

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose **iwtm-siem** option.
4. Choose **DB siem user** option.
5. Choose **DB audit logging management** option.
6. Set parameters:

| Parameter | Description |
|---|---|
| `Enter login for DB administrative account` | Login of Oracle/Postgre administrators account |
| `Enter password for DB administrative account` | Password of for Oracle/Postgre administrators account |

7. Press **Check logging status**.

8. When:
    - **DB audit logging to OS journal: OFF** - press **Change logging status**, to enable logging.
    - **DB audit logging to OS journal: ON** - press **Change logging status**, to disable logging.

## Managing siem user

This chapter describes creating, deleting and changing password for **siem** user, which is used by SIEM to interact with Traffic Monitor:

- Creating siem user;
- Changing siem user password;
- Deleting siem user.

## Creating siem user

**To create siem user**:

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose **iwtm-siem** option.
4. Choose **DB siem user** option.
5. Choose **CreateDB siem user** option.
6. Set parameters:

| Parameter | Description |
|---|---|
| `Enter login for DB administrative account` | Login of Oracle/Postgre administrators account |
| `Enter password for DB administrative account` | Password of for Oracle/Postgre administrators account |
| `Enter password DB siem user` | Password for new **siem** user |

7. Press **Create**.

## Changing siem user password

**To change siem user password:**

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose**iwtm-siem** option.
4. Choose **DB siem user** option.
5. Choose **Change password for DB siem user** option.

6. Set parameters:

| Parameter | Description |
|---|---|
| `Enter login for DB administrative account` | Login of Oracle/Postgre administrators account |
| `Enter password for DB administrative account` | Password of for Oracle/Postgre administrators account |
| `Enter new password user siem` | New password for **siem** user |

7. Press **Change password**.

## Deleting siem user

**To delete siem user:**

1. Go to **setup** utility from TM command line, by using `setup` command.
2. Choose **IW Services configuration** option.
3. Choose**iwtm-siem** option.
4. Choose **DB siem user** option.
5. Choose**Delete DB siem user** option.
6. Set parameters:

| Parameter | Description |
|---|---|
| `Enter login for DB administrative account` | Login of Oracle/Postgre administrators account |
| `Enter password for DB administrative account` | Password of for Oracle/Postgre administrators account |

7. Press **Delete**.

## 7.11.3 Type of logs, transmitted to SIEM

Rsyslog forms commen system journal. It is a protocol, which is used to transmit logs to SIEM.

There are five major log types, transmitted to SIEM:

1. **iw_*** processes logs. For example:
```
Mar 11 14:32:30 iw-VMware-4224da3ab iw_expressd: 5 (18485:0x00007f53001b97e0)
[INFO   ] : <Root> Runtime environment initialized. Starting...
```

2. **pguard** script logs. Script monitors state of services and restarts them when necessary:
   ```
   Mar 11 14:32:26 iw-VMware-4224da3ab pguard: 148 (18256:0) [INFO] : expressd
   Terminating pid 18257 (signal 15)
   ```
3. Logs of login and logout of **Oracle DB**:
   ```
   Mar 11 14:28:20 iw-VMware-4224da3ab Oracle Audit[17786]: LENGTH : '153' ACTION :[7]
   'STARTUP' DATABASE USER:[1] '/' PRIVILEGE :[4] 'NONE' CLIENT USER:[4] 'root' CLIENT
   TERMINAL:[13] 'Not Available' STATUS:[1] '0' DBID:[0]
   ```
4. **Linux users** login and logout:
   ```
   Mar 11 14:32:02 iw-VMware-4224da3ab runuser: pam_unix(runuser:session): session
   opened for user iwtm by root(uid=0)
   ```
5. **Nagios** logs:
   ```
   Feb 10 20:05:39 iw-VMware-4224289a4 nagios: SERVICE ALERT: IWTM;TM_DAEMONS_STATE;
   CRITICAL;SOFT;1;CRITICAL - updater(3)
   ```

# 7.12 Deleting temporary files

Ability to delete temporary files has been implemented in the product as **clean_temporary_files.sh** script.

Script deletes the following information:

1. Files from operation system's temporary directory (`/opt/iw/tm5/tmp/` directory).
2. Data from Traffic Monitor file queue directory (`/opt/iw/tm5/queue/` directory).

> **Note:**
>
> New events will not be processed by the system during temporary files deletion. Information about all unprocessed data will be deleted at the moment of script execution.

**To delete temporary files**:

1. Run **clean_temporary_files.sh** script:
   ```
   /opt/iw/tm5/bin/clean_temporary_files.sh
   ```
2. Accept temporary files deletion:
   ```
   yes
   ```

# Appendix A. User Name and Password recommendations

### 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:
    - o Include whole words or phrases into a password.
    - o Use a series of the same character.
    - o Start and end the password with the same character.
    - o Create a new password by adding characters to your current password

### General recommendations

Do not start usernames 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 B. Monitoring indicators

The following table lists all indicators that are used by monitoring subsystem for checking state of the System components. The check includes obtaining an indicator value at regular intervals and comparing it with a threshold value.

> **Warning!**
>
> If configuration files have been changed, threshold values and the check period may differ from the specified values.

Critical values of all indicators may signal that the servers being checked are physically inaccessible. In this case, please check the servers' performance.

Service management (e.g., the status check) is performed from a root account.

> **Warning!**
>
> If recommendations from the table below did not help you to solve the problem, please contact InfoWatch technical support at support@infowatch.com.

| Indicator name | What is checked | Values | Poll interval |
|---|---|---|---|
| System load | Load of IW-Linux-servers, TMcap-servers, DB-servers over the last 15, 5 and 1 minute | – at least one figure exceeds the value of 20.0,16.0 and 12.0 for 15, 5 and 1 minute respectively<br>– at least one figure exceeds the value of 10.0,8.0 and 6.0 for 15, 5, and 1 minute respectively<br>– none of the figures exceeds the value of 10.0,8.0 and 6.0 for 15, 5 and 1 minute respectively | 30 minutes |
| Current users | The number of users registered at the host | – > 50 users<br>– from 20 to 50 users | 30 minutes |

| Indicator name | What is checked | Values | Poll interval |
|---|---|---|---|
| | | – < 20 users | |
| DB Alert Log Errors | Whether Alert Log contains errors | – errors found<br>– no errors | 5 minutes |
| Server availability | Availability of Linux servers | – > 500 milliseconds<br>– from 100 to 500 milliseconds<br>– < 100 milliseconds | 5 minutes |
| Postfix server availability | Availability of Postfix server | – not available<br>– available | 30 minutes |
| SSH availability | Checks whether a SSH service is available for a specified server group | – >= 10 seconds<br>– < 10 seconds | 10 minutes |
| Availability of Device Monitor server | Checks whether Device Monitor server is available<br>**Warning!**<br>Perform the following steps to configure the indicator:<br>1. Uncomment Device Monitor section in the configuration file **/etc/nagios/iwmon/iwmon-hosts.cfg** and specify a correct IP address instead of `<hostname>`.<br>2. Uncomment Device Monitor section in the configuration file **/etc/nagios/iwmon/iwmon-commands.cfg**<br>3. Uncomment commented lines in the configuration file **/etc/nagios/iwmon/iwmon-services-dm.cfg**<br>4. Make sure that configuration files do not contain errors:<br>`nagios -v /etc/nagios/nagios.cfg`<br>5. Restart the Nagios service: `service nagios restart` | – no connection<br>– connection established | 30 minutes |
| Swap usage | Free swap space (virtual memory) | – < 10% free | 5 minutes |

| Indicator name | What is checked | Values | Poll interval |
|---|---|---|---|
| | | – from 10 % to 20% free<br>– > 20% free | |
| Root Partition free space | Free space in the root file system | – < 10 000 MB<br>– from 10 000 MB to 20 000 MB<br>– > 20 000 MB | 30 minutes |
| Var Partition free space | Free space in /var file system | – < 10 000 MB<br>– from 10 000 MB to 20 000 MB<br>– > 20 000 MB | 30 minutes |
| NTP status | Availability of time synchronization service | – NTP server is available<br>– NTP server is unavailable | 30 minutes |
| NTP time deviation | Time lag on the System servers and NTP server<br>**Note:**<br>If the System cannot establish connection with NTP servers or NTP servers are not specified in the System configuration, the following error message will occur “can't create socket connection”.<br>In this case, make sure that a correct value for NPT server is specified in the ntp.conf and iwmon-services-ntp.cfg configuration files and that the value in both files is the same. | – > 40 seconds<br>–from 20 to 40 seconds<br>– < 20 seconds | 360 minutes |
| Core dump | Checks services’ operation for crashes | – no core dumps<br>– core dump | 30 minutes |
| Database Status | Checks database state for a specified SID. A standard Nagios plugin in used. | – ok<br>– <> ok | 10 minutes |
| Oracle TNS Status | Status of Oracle DB access service | – TNS listener is started | |

| Indicator name | What is checked | Values | Poll interval |
|---|---|---|---|
| | | – TNS listener is not started | 10 minutes |
| Main partition DB free space | Free space on the partition that stores main information (By default: `/u01`) | – < 10 000 MB<br>– from 10000 to 20 000 MB<br>– > 20 000 MB | 30 minutes |
| Data partition free space | Free space on partitions that store events (By default: `/u02`) | – < 7%<br>– from 7 to 15%<br>– > 15% | 30 minutes |
| Oracle patch status | Whether Oracle patches 17402822 and 12919564 are installed. These patches are needed for correct operation of the System | – not installed<br>– installed | 30 minutes |
| DB Alert log Size | Size of Alert Log file | – > 100 MB<br>– from 50 to 100 MB<br>– < 50 MB | 5 minutes |
| DB sys log errors | Checks database syslog whether there are errors for iwtm schema | – errors found<br>– no errors found | 30 minutes |
| Total Processes | Retrieves the number of running processes | – > 600 processes<br>– from 450 to 600 processes<br>– < 450 processes | 30 minutes |
| State of syslog service | Checks whether the syslog service is started | – service not available | 30 minutes |

| Indicator name | What is checked | Values | Poll interval |
|---|---|---|---|
| | | – service availalbe | |
| SMTP queue | Measures the speed of processing objects by IW_MESSED service. Objects are placed to the queue by IW_SMTPD and IW_PROXY services (smtp). Retrieves the number of objects in the queue | – > 10000 objects<br>– from 1000 to 10000 objects<br>– < 1000 objects | 30 minutes |
| Queue for loading events to storage | Speed of loading events to database (objects placed to the queue by IW_XML2LIRO service are processed by IW_LOADER service). Retrieves the number of objects in the queue | – > 10000 objects<br>– from 1000 to 10000 objects<br>– < 1000 objects | 30 minutes |
| Processing errors queue | The number of objects processed with errors by the services IW_EXPRESSD, IW_MESSED, IW_PROXY (http, icq), IW_ICAP. Retrieves the number of objects in the errors queue | – > 1000 objects<br>– from 200 to 1000 objects<br>– < 200 objects | 30 minutes |
| Indexing queue | Queue of objects for indexing in Sphinx for full-text search | – > 10000 objects<br>– from 1000 to 10000 objects<br>– < 1000 objects | 30 minutes |
| Indexing errors | Number of errors occurred when indexing events by **iw_indexer** service | – > 50 errors<br>– from 1 to 50 errors<br>– < 50 errors | 30 minutes |
| Applied policies actions processing errors queue | Number of applied policies actions processing errors | – > 50 errors<br>– from 1 to 50 errors<br>– < 50 errors | 30 minutes |

| Indicator name | What is checked | Values | Poll interval |
| --- | --- | --- | --- |
| Applied policies actions processing queue | Applied policies actions processing queue | – > 1000 objects<br>– from 200 to 1000 errors<br>– < 200 errors | 30 minutes |
| **iw_loader** and **iw_xml2liro** processing errors queue | **iw_loader** and **iw_xml2liro** processing errors queue | – > 50 errors<br>– from 1 to 50 errors<br>– 0 | 30 minutes |