



# Administrator's Guide

**Internet Administrator for Network**  
**Version 3.5 update #20**

<b>SECTION 1 - INTRODUCTION .....</b>	<b>4</b>
SECTION 2.1. - SYSTEM REQUIREMENTS .....	5
SECTION 2.2 - BEFORE INSTALLATION .....	5
SECTION 2.3. - INSTALLATION PROCESS .....	7
SECTION 2.4. - COMPONENTS OF INTERNET ADMINISTRATOR .....	14
<b>SECTION 3 - SYSTEM SETTINGS.....</b>	<b>17</b>
SECTION 3.1. - SETTING THE NETWORK PARAMETERS.....	17
SECTION 3.2. - SETTING THE IADMIN PROXY .....	19
SECTION 3.3. - SETTING THE USER LOGIN MODE .....	21
SECTION 3.4. - CUSTOM MONITORED TCP/UDP PORTS.....	22
SECTION 3.5. - WEB SITE MONITORING VIA PACKET ENGINE.....	22
SECTION 3.6. - ADVANCED SETTINGS .....	23
<b>SECTION 4 - USER MANAGEMENT.....</b>	<b>24</b>
SECTION 4.1. - USERS, GROUPS, AND COMPUTERS .....	24
SECTION 4.2. - INTERNET ACCESS LOG .....	31
SECTION 4.3. - IADMIN WEB - STATISTICS AND USER LOGIN.....	33
<b>SECTION 5 - INTERNET ACCESS CONTROL.....</b>	<b>36</b>
SECTION 5.1. - A SET OF RULES .....	36
SECTION 5.2. - HOW DO THE RULES .....	37
SECTION 5.3. - ELEMENTS OF THE RULE .....	38
<b>РАЗДЕЛ 6 – SERVICE.....</b>	<b>45</b>
SECTION 6.1. – LICENSING .....	45
SECTION 6.2. - LICENSING URL CATEGORY DATABASE.....	46
SECTION 6.3. – URL CATEGORY DATABASE UPDATE.....	47
SECTION 6.4. - UNMONITORED WORKSTATIONS .....	48
SECTION 6.5. - PURGE DATABASE .....	49
SECTION 6.6. - CUSTOM SITES IN CATEGORY .....	50
SECTION 6.6. – USERNAME SEARCH.....	51
<b>SECTION 7 - REPORTS .....</b>	<b>52</b>
SECTION 7.1. - REPORTING.....	52
SECTION 7.2. - CUSTOMIZED REPORTING .....	52
SECTION 7.3. - LIST OF REPORTS.....	53
SECTION 7.4. - EXPORT DATA TO THE W3C.....	53
<b>SECTION 8 - DATABASE AND MICROSOFT SQL SERVER .....</b>	<b>54</b>
SECTION 8.1. - THE DEFAULT DATABASE .....	54
SECTION 8.2. - MS SQL SERVER DATABASE .....	55
SECTION 8.3. – BACKUP.....	59
<b>SECTION 9 - DISTRIBUTED NETWORK AND COLLECTORS.....</b>	<b>60</b>
SECTION 9.1. - CENTRAL DATA WAREHOUSE.....	60
SECTION 9.2. - INSTALLATION OF ADDITIONAL COLLECTORS .....	60
SECTION 9.3. - ADMINISTRATION .....	61



## SECTION 1 - INTRODUCTION

"Internet Administrator for Network" is a software for complete Internet access control at any network.

"Internet Administrator" provides:

- internet monitoring
- content filtering
- traffic and time control
- access control to categories, web sites, domains, protocols, content types and more.

Access control is based on a flexible system of rules. Content filtering is based on IAdmin URL category database. " Internet Administrator for Network " contains report system with more than 10 reports for detailed internet statistics.

## SECTION 2 - INSTALLATION

### Section 2.1. - System requirements

#### Operation system:

Windows 7; Windows 7 Service Pack 1; Windows 8; Windows 8.1; Windows Server 2008 R2; Windows Server 2008 R2 SP1; Windows Server 2012; Windows Server 2012 R2

**CPU:** x64 Intel-compatible processor with a minimum speed of 1 GHz or a faster processor

**Memory:** 2048mb minimum, 4096mb recommended.

**Space on a hard drive:** 4.2 GB of Disk Space.

#### Other:

- Network card with promiscuous mode enabled. All network adapters support this mode by default but it can be disabled in adapter settings.
- The absence of the network software, firewalls that can restrict the flow of network packets that are not sent for the local server, see <http://www.iadmin.biz/products/?pid=40>.
- Microsoft .Net Framework 3.5 SP1 enabled or Microsoft .Net Framework 4.0 installed.

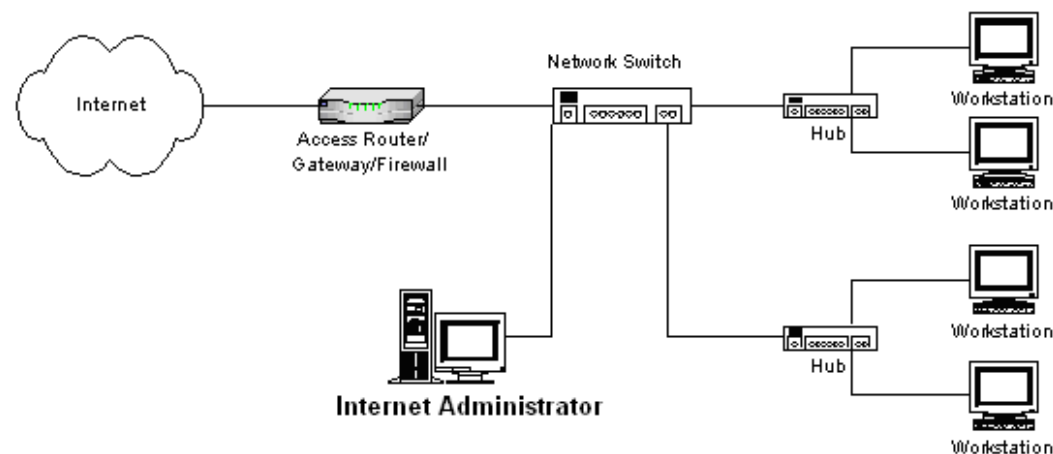
#### Internet Administrator must be installed on the server that is:

- Connected to a mirroring port of network switch or router
- Or acting as the Internet gateway.
- Or Microsoft TMG Server 2010

### Section 2.2 - Before installation

The location of Internet Administrator server in a network is important because it captures network packets directly from network card. To see all traffic from workstations to the Internet it must be installed on mirroring port of network switch or on Internet gateway.

#### Variant 1 - Mirroring port of network switch



This network is based on managed network switch which supports port mirroring. On a managed switch it is possible to configure port mirroring, and to specify the port to which Internet Administrator server is connected as monitoring port, and a port through which the Internet traffic goes as mirrored port. Thus all Internet traffic will be copied to Internet Administrator server for analysis.

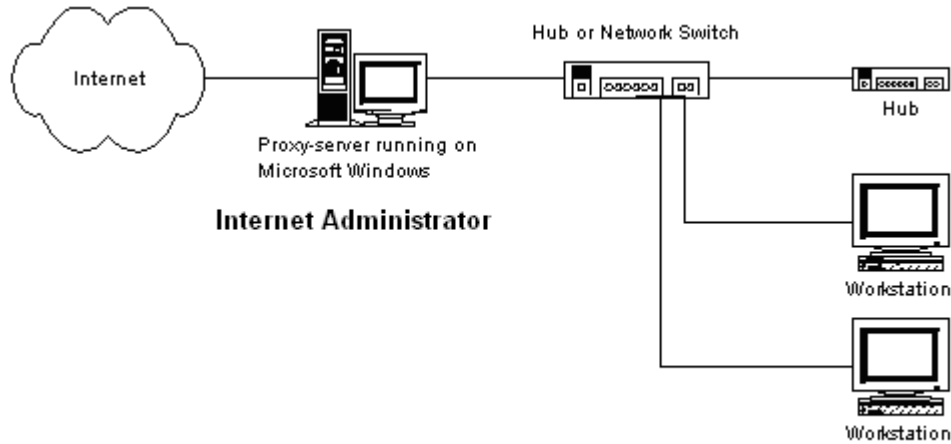
Blocking TCP connections is carried out by sending special packets. In some managed switches, for example, CISCO, when configuring port mirroring, it denies to send outgoing packets on this port. So server connected to this port will not work in the network and Internet Administrator can only monitor traffic but not block. In this case, use a second network card

Copyright © 2015 Internet Administrator Company Ltd.

<http://www.iadmin.biz>, e-mail: [sales@iadmin.biz](mailto:sales@iadmin.biz)

on the server that is connected to a common port (non-mirroring). Second card must be configured in Options of Internet Administrator to block connections.

#### **Variant 2 - Internet Gateway**



If workstations are connected to the Internet through the router, proxy server or network address translator (NAT) on the Windows platform, the installation can be done on this server.

However, with some programs there is an incompatibility. More about them <http://www.iadmin.biz/products/?pid=40>

If Microsoft TMG Server 2010 is used Internet Administrator integrates with it while installing. In TMG mode Internet Administrator gets traffic from TMG Server only, not from network segment.

#### **Variant 3 - Network Bridge**

Small networks usually connected to the internet using hardware gateway when the network has a single unmanaged switch that is connected to the Internet channel and other computers. There is a method of converting the network to Variant 2 without using additional software and without rebuilding of the logical network. This is accomplished with using the network bridge between 2 or more network cards in Microsoft Windows. The bridge is not the gateway or router and allows all traffic through itself, so other computers do not need to reconfigure TCP/IP settings.

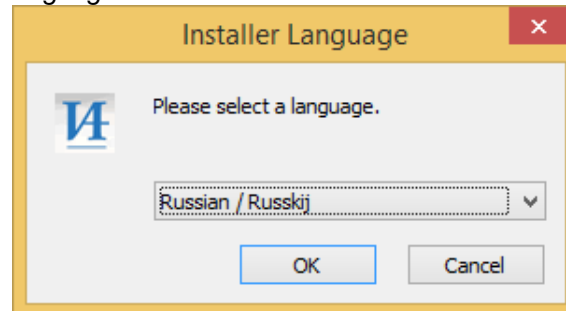
To create the network bridge, do the following:

- Choose a computer from your network with MS Windows which will be Internet Administrator server.
- Install the second network card into the server if not present.
- Disconnect the Internet cable from the network switch and connect it to a new network card.
- In the properties of a network environment choose two network cards and in the context menu specify Bridge Connections.
- Set IP address and other TCP/IP parameters that the first network card had to the created bridge.
- Check the Internet from the server and from other workstations.
- Install Internet Administrator on the server.
- If the server will be shutdown, other workstations will not get access to the Internet.

### Section 2.3. - Installation process

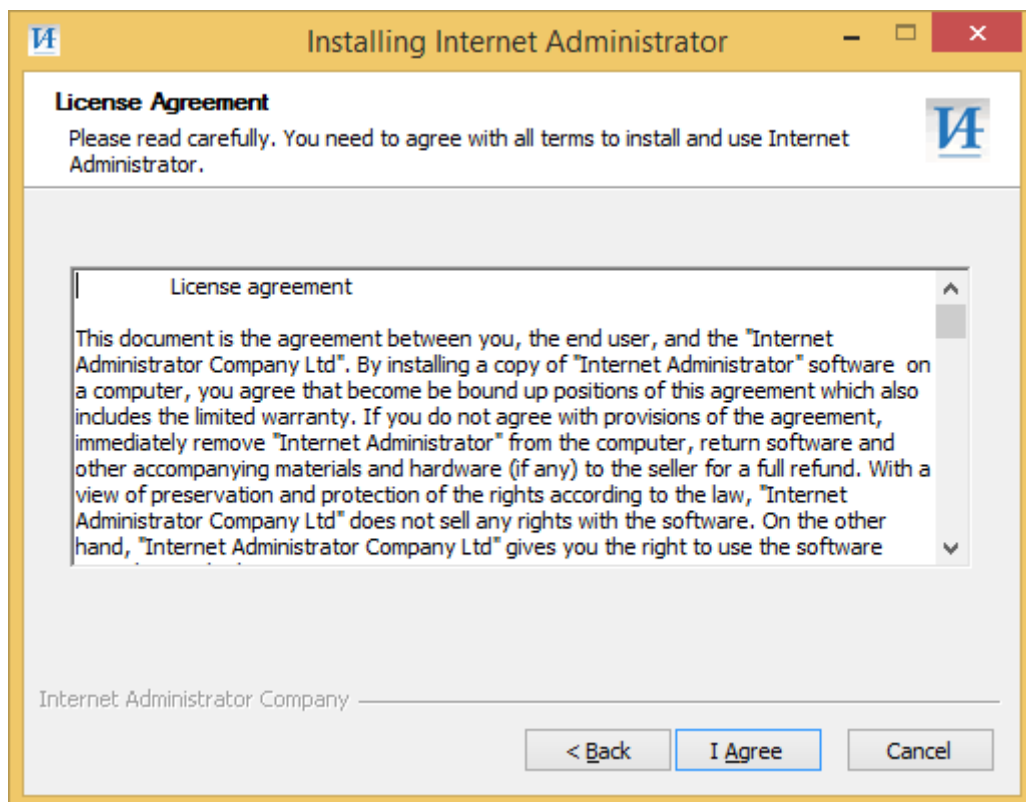
To start the installation, run the setup file that you downloaded from the site. During the installation, you walk a few steps, which you will be prompted to enter the necessary data, or read the information.

#### Step 1 - Select the language



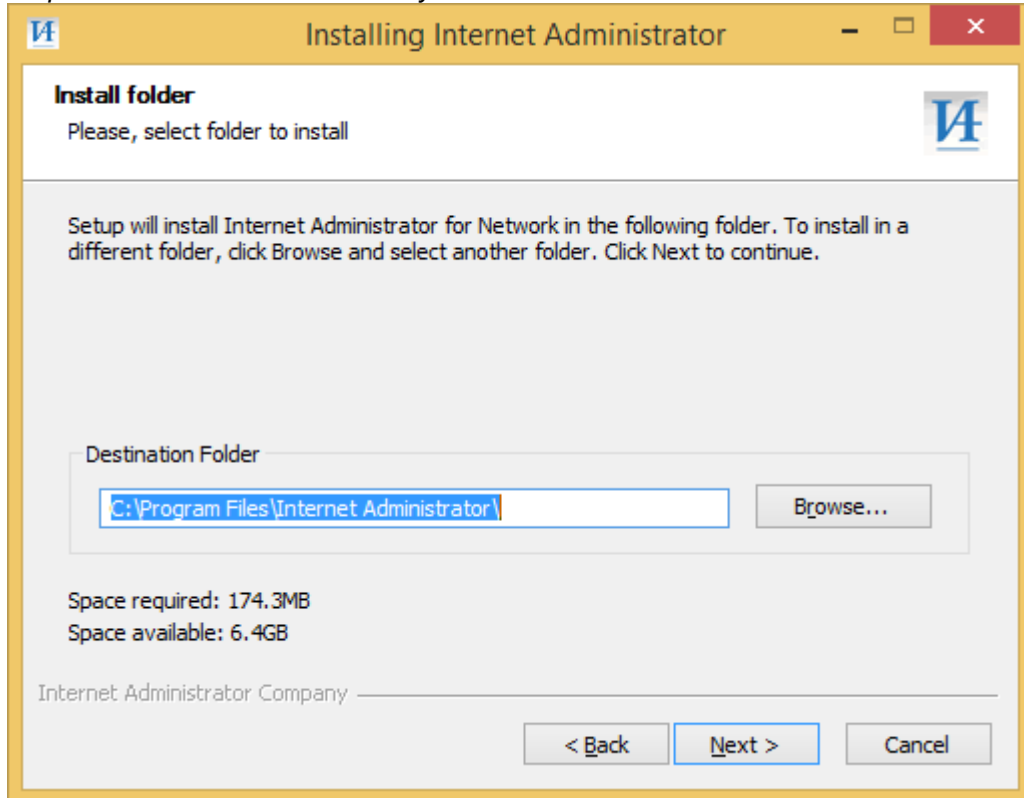
Internet Administrator can be set to English or Russian. Choice of language would be available if the system has a multi-language support. If you have an English version of Windows and is not configured to use the default language for non-Unicode programs, the program will be set in English only.

#### Step 2 - The license agreement



Read the license agreement, which regulates the use of software and responsible manufacturer and user. To continue the installation, you must accept the license agreement by clicking "Accept"

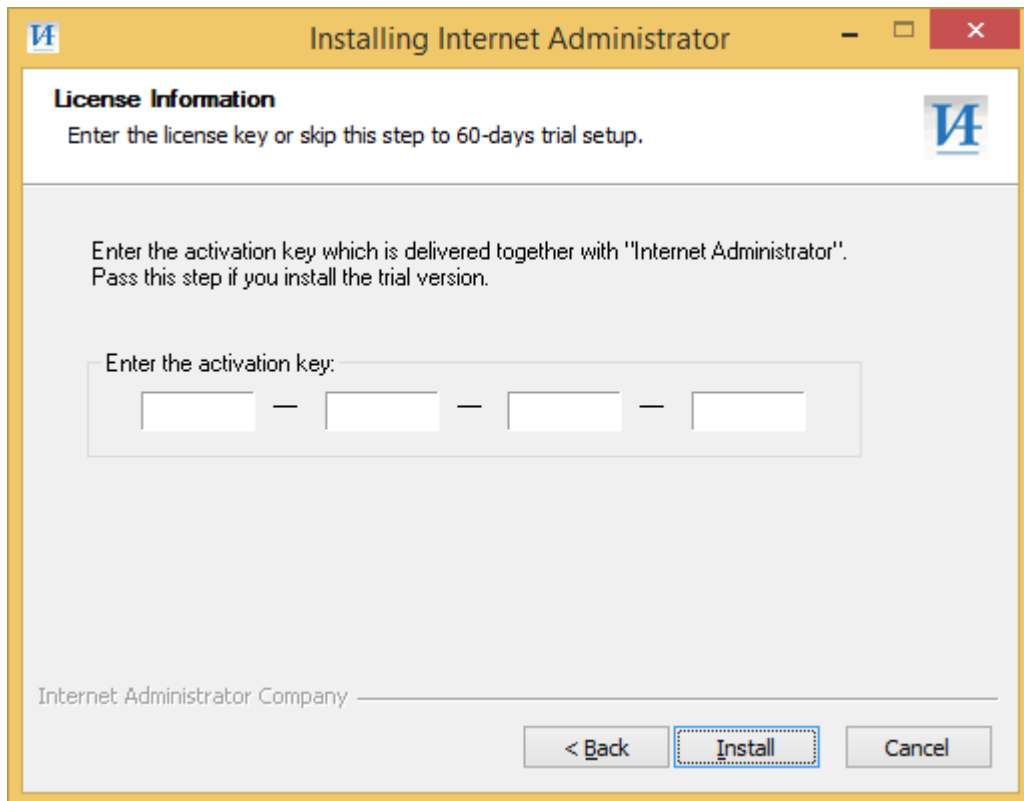
*Step 5 - Select Installation Directory*



Select the directory in which you want to install "Internet Administrator". By default, the installer will prompt you to install the software in a subdirectory Internet Administrator directory software Windows, such as, C: \ Program Files \ Internet Administrator.

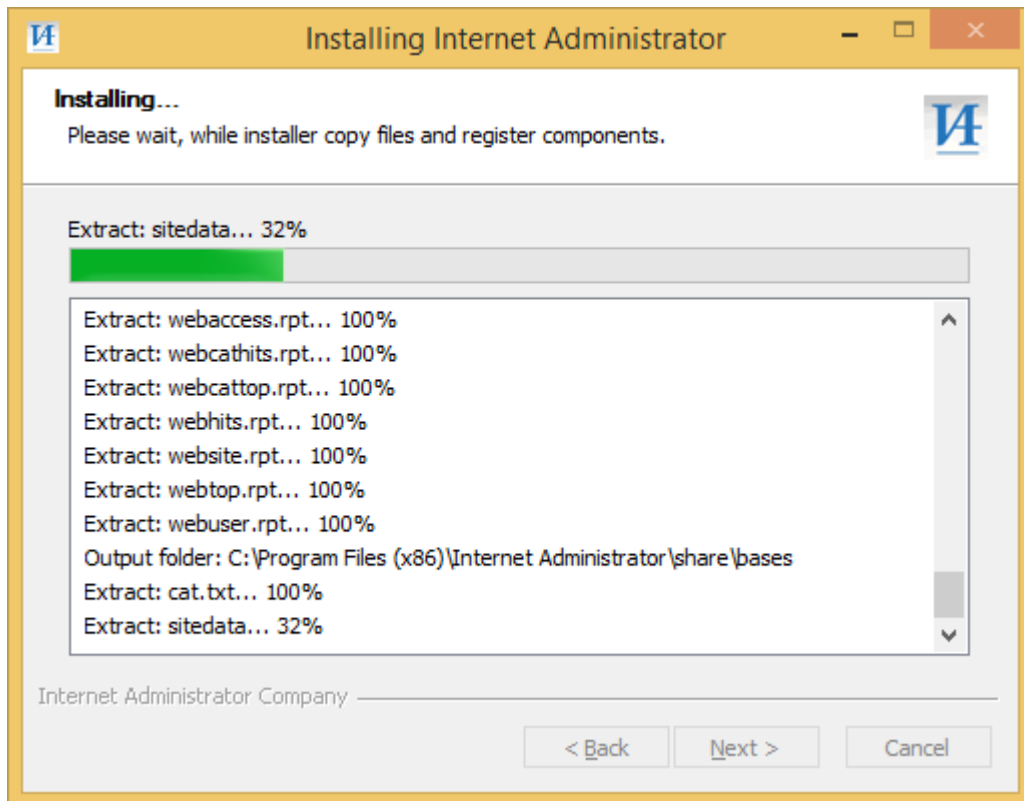
*Step 4 - Enter the license key*





If you purchased a copy of the software "Internet Administrator", at this stage, you should enter the license key obtained after purchasing the program. Verifying the key here is not carried out. If you install the "Internet Administrator" in the test mode, then enter the key is not necessary. However, the "Internet Administrator" will run 60 days from the date of installation and the service will cease to run. Enter the license key, you can at any time after installation.

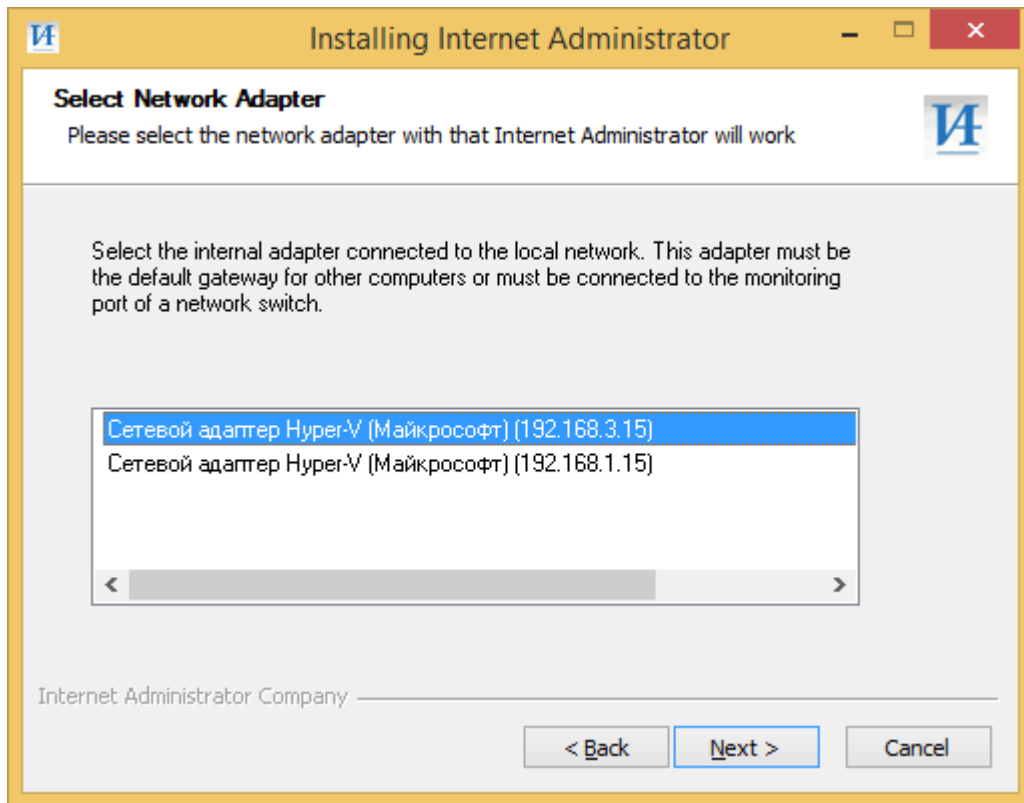
*Step 5 - Copying of files, registration of components*



At this stage the installer copies all necessary files to the system folder and the "Internet Administrator" folder, registers libraries and DCOM components, installs the driver and system services.

The installer will install the free Microsoft SQL Server Express 2014 as a DBMS and create a new database. If this process fails the installation of Microsoft SQL Server and creation a new database you must perform manually. See Section 8 - DATABASE AND MICROSOFT SQL SERVER.

Step 6 - Selecting the network adapter to bind



"Internet Administrator" will monitor the traffic passing through only one network segment connected to the selected network adapter. You should select the adapter that connected with to the internal network. If you configured port mirroring, then select the adapter connected to mirroring port. This setting does not affect in Forefront TMG mode.

*Step 7 - Entering the pool of local IP-addresses*

The screenshot shows a window titled "Installing Internet Administrator" with a yellow header bar. Inside, the "Network Settings" section asks the user to specify the local address of their network. It includes a table for the local network list, input fields for IP network and mask, and fields for the server's IP address and port. The "Next >" button is highlighted with a dashed border.

IP network	Subnet mask
192.168.1.0	255.255.255.0

IP network (eg. 192.168.0.0):

Mask (eg. 255.255.255.0):

Enter the IP address of this server and port that the web server will use.

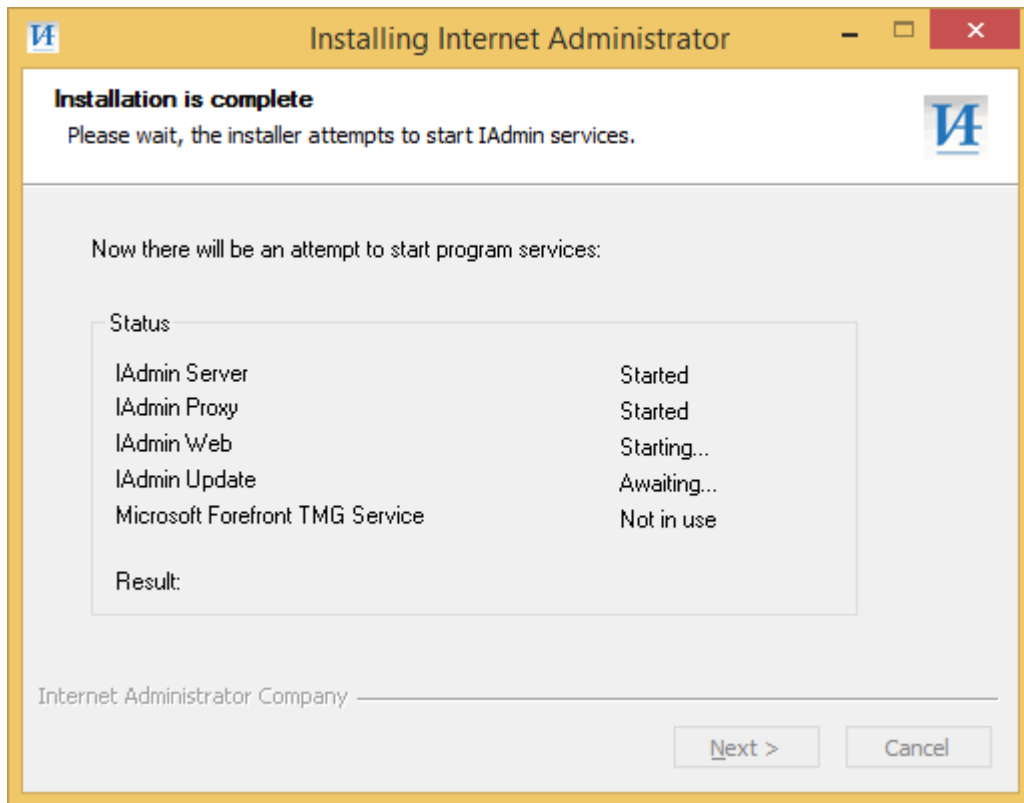
IP address:  Port:

Internet Administrator Company

The installer found the initial address taken from the selected network adapter. However, you can change them during the installation. You must enter the IP network and mask according to the TCP/IP rules, which define your network. You can change these settings after installation.

There is also need to specify the address and port of the IAdmin Web server. As an address must be specified IP address of the server is available for network computers. As a port it can be specified any unused TCP port.

*Step 8 - Attempt to start the services*



In the final step of the installation the program makes an attempt to start drivers and services. In most cases, installation is successful, and you can begin working immediately thereafter. However, in case of failure, you need to analyze the Windows event log for the cause.

If the installer detects a previous version of the program, it will ask to remove it before installing the next. With this you can save the database iadmin.mdb with all information and then replace it after a new installation. If you are using a database to MS SQL server, then after installation use "Database Wizard" to select a working database. **WARNING! Version 3.5 will only compatible with database from version 3.0, update 20 and if database located on MS SQL Server!**

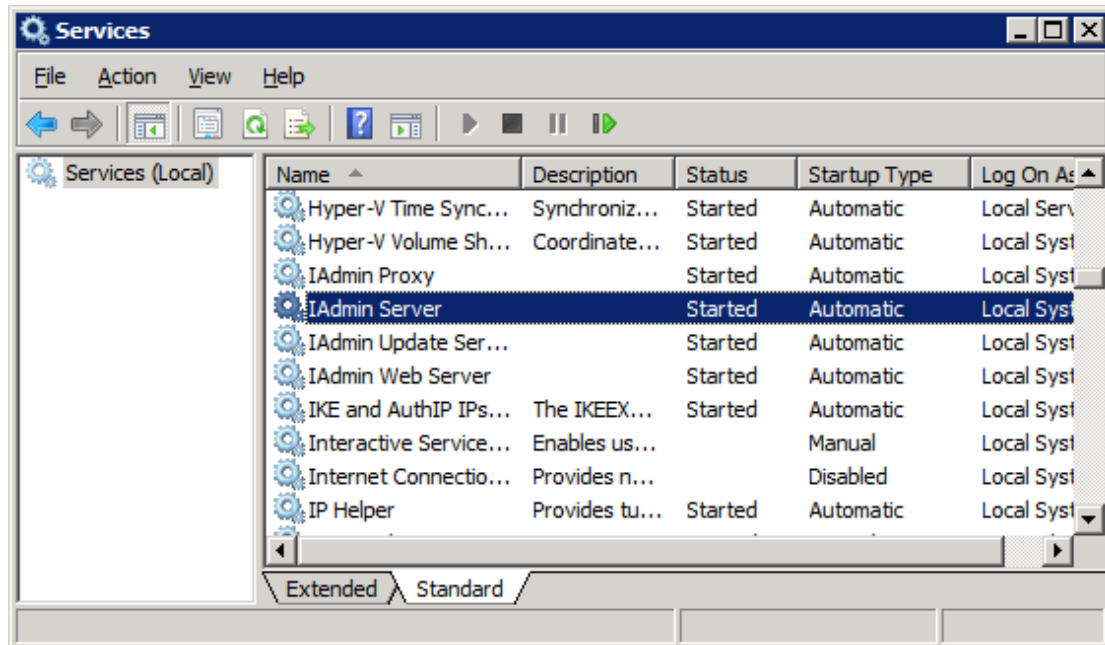
**Note.** Starting with update 17, the program provides its own HTTP\HTTPS proxy server IAdmin Proxy. If you have a **third-party** proxy server on a **same** server, reconfigure its clients to use IAdmin Proxy.. If you have a **third-party** proxy server on a **separate** server, its internal IP address used for user inquiries must be excluded from local networks using the administrative tools "Rules Admin" (Tools -> Settings -> Network tab).

**After installing "Internet Administrator" is working in a static mode and detects new users and computers automatically. The workstation must perform any request to the Internet for detection. If new users do not appear after a few minutes after installation, check whether proper the network adapter is selected and whether proper local IP network is specified.**

## Section 2.4. - Components of Internet Administrator

After installation the server will contain the following system components:

1. Iadmin Packet driver named NPF (file npf.sys) – it works with the network card driver and monitors network packets.
2. Windows Services:



- IAdmin Server performs most of the work on monitoring and access control. If this service is not running, the program does not work. The service stops at the end of the trial period and it cannot be started without the license key input. The service creates a process iadmindsv.exe, which can take up a large amount of memory, up to 300 megabytes and more. This amount of memory is required to load a URL category database with 4 million sites.

- IAdmin Proxy - HTTP / HTTPS proxy server. By default, accepts requests from clients on all IP addresses of the server on port 8080 (8081 in Forefront TMG mode). Performs processing TLS / SSL traffic using own certificates, enables decrypt HTTPS, handles content types and more detailed parameters of the HTTP protocol.

- IAdmin Update Service is a service, which is engaged in updating the Iadmin URL category database, as well as cleaning of the main database on a schedule. It creates a process iadminupdateservice.exe and makes log to update.log file in the installation folder.

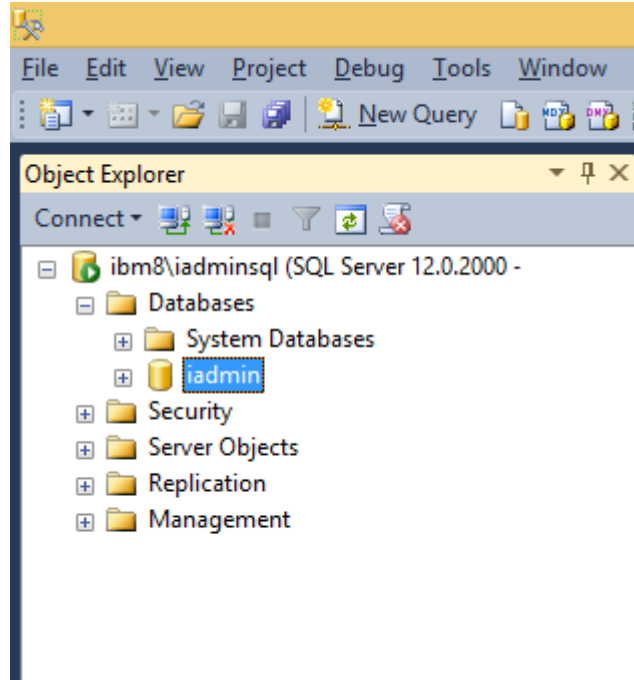
- IAdmin Web Server is a web server to display statistics for users and to implement registration of users in the MS Active Directory mode and the Username & password mode. Creates a process IAdminWebSvc.exe.

### 3. Main database.

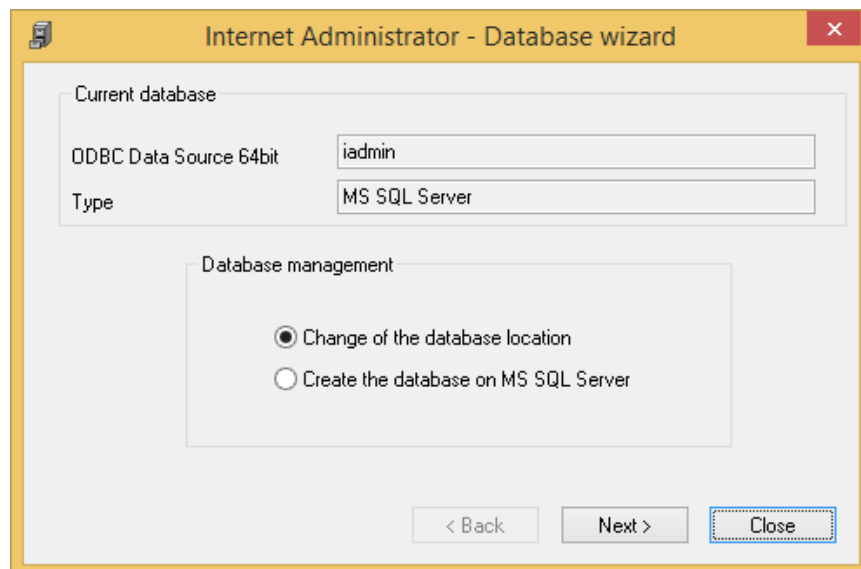
Version 3.5 uses as its default database free Microsoft SQL Server Express 2014.

To access the database requires additional installation of Microsoft SQL Server Management Studio, available for download from Microsoft.

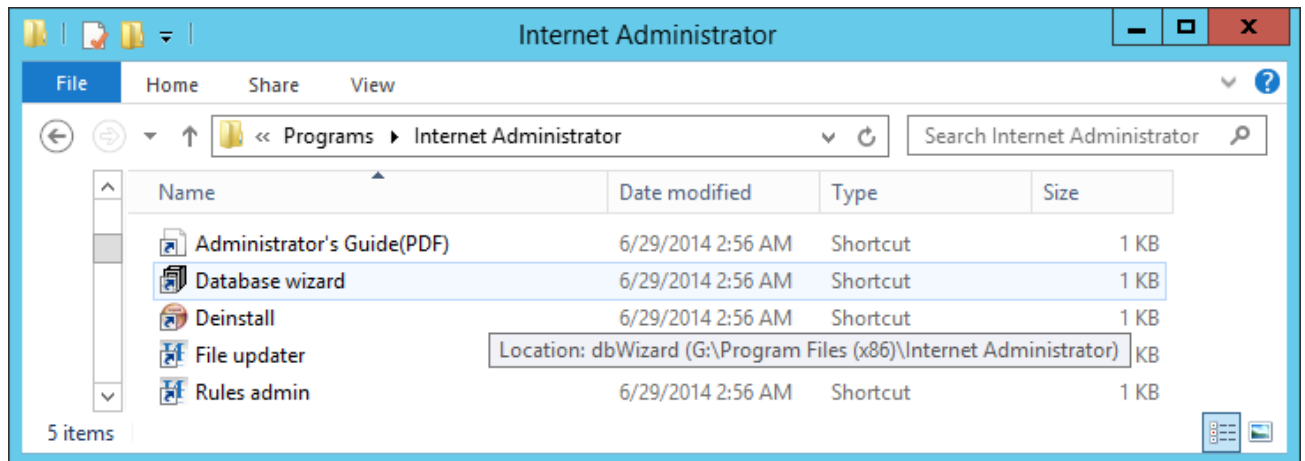
The database instance is ADMINSQL on a local server (SQL Server name: localhost \ iadminsql). A Windows user on whose behalf the program is being installed is an administrator of the instance IADMINSQL.



To manage the main database, use Internet Administrator Database to create a new database on MS SQL Server, or to change its location, SQL user and SQL password.



4. Internet Administrator Program Group.



Here are the management tools that are available to run from the Start menu> All Programs or Start-> Applications (in Windows 8 and Server 2012).

"Rules Admin" is a main management utility which specifies all settings, monitors sites and users and creates an access rules.

"Database wizard" is a program for changing main database type and location and creating the database on Microsoft SQL Server.

"File updater" is a program to automatically update the Internet Administrator program files. When you run the Rules Admin, it checks for new updates and starts Update files when a new version of the program is available.



## SECTION 3 - SYSTEM SETTINGS

Setting up the system is performed using the "Rules Admin".

### Section 3.1. - Setting the network parameters

"Internet Administrator" has two parameters directly affect the operation of the system. They are the network card to which the service is bound and the list of local IP networks. When these parameters are set incorrectly, the system will not work as needed.

#### Network Cards

Bind to the network card is done in the menu Service-> Select network card.

Binding should be implemented to the card, through which Internet traffic goes from users' computers to the Internet. If you have a gateway (router, NAT, proxy server) with two or more network adapters, the binding should be to an internal card that is connected to the LAN. If the gateway is a network bridge, binding may be done to the external card.

If you use a managed switch, which prohibits sending packets through mirroring port, to work the blocking mechanism you need to use a second network card connected to a normal port and to select it as a separate adapter to block. In this case, the OK button is available only when both cards are selected.

Network card

Network card to work: Network Adapter Hyper-V

IP address: 192.168.1.15

Select network card to work:

☐ Use different network card to send blocking packets

Network card to send:

IP address:

Select network card to send packets:

Use different card to send blocking packets if your network device disables packet sending on mirroring port. If using different card for blocking, disable (uncheck) any protocols and services on working card.

OK Cancel

## Local IP Networks

Setup of local IP networks is done in the menu Service-> Options at the Network settings property page.

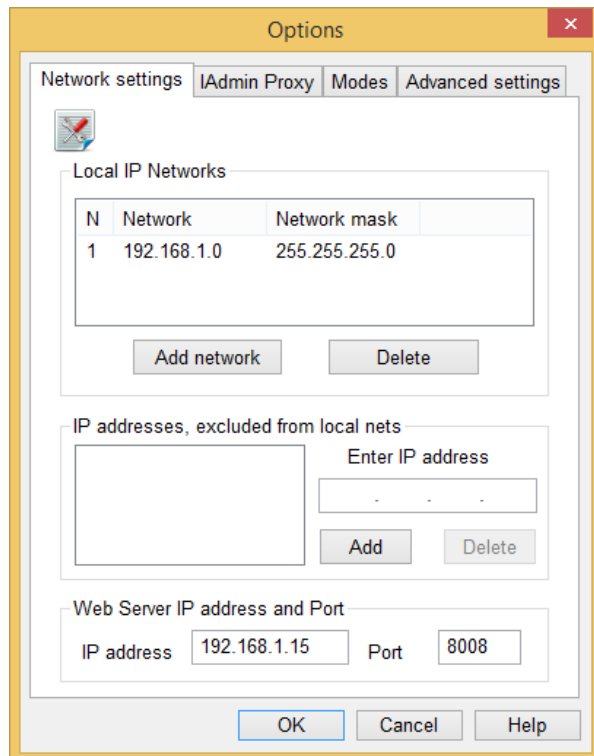
Local IP networks define a set of IP addresses which belong to your internal network. Network Address consists from IP network address (not a host!) and a network mask. You can set up to 10 various IP networks.

The IP addresses excluded from the local IP networks are external, that is Internet addresses. Any query to such addresses will be logged as an access to the Internet. The purpose of such addresses is necessary when a third-party proxy server is used in your network, except IAdmin Proxy. Its internal IP address needs to be added to the list of excluded IP addresses.

If the DNS server is located inside the local network, they also need to be excluded that "Internet Administrator" could properly resolve the names of hosts that are accessed is on protocols other than HTTP.

## IAdmin Web Server

IP address of the Web server must belong to a server that is running Internet Administrator, and be accessible to internal users. Web requests will be redirected to this address for authentication, if the user is not registered. Port defines the TCP port on which the web server listens for requests. This port must not be used by other programs! **If you use a proxy server, the address of IAdmin Web server must be added to the exclusion of "Do not use proxy server for local addresses" or "Do not use proxy server for addresses beginning with".**



### Section 3.2. - Setting the IAdmin Proxy

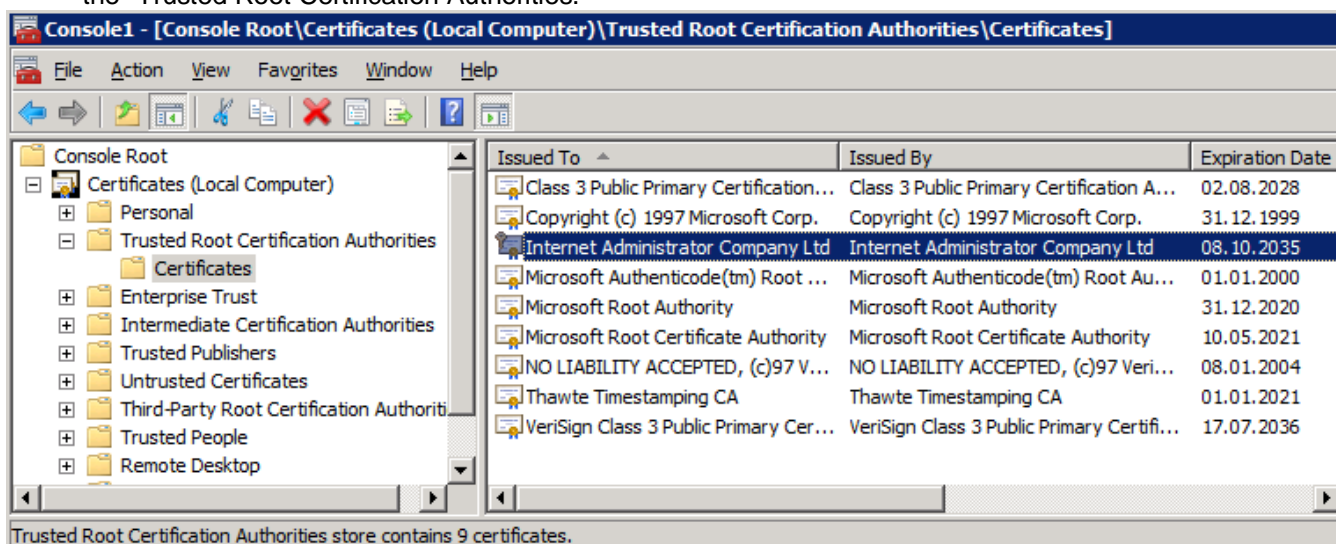
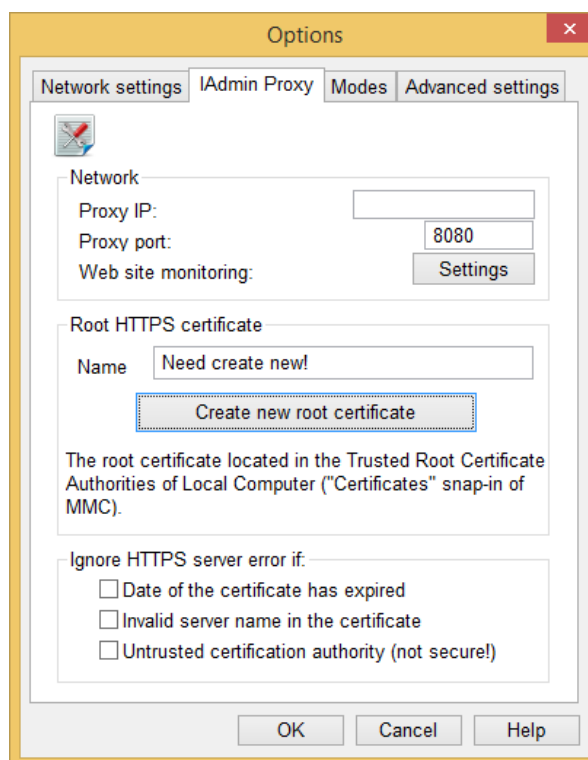
Admin Proxy is an independent network component to collect traffic. Its internal IP address, which connect clientss must belong to the local subnets, and the external IP address from which the requests to the Internet from the server - must not. If the server with IAdmin Proxy has one network card, you need to logically separate it by two subnets: for the internal network and external, which is set to the default gateway. If you use two network cards, the subnet on the external network card simply has to be absent from the list of local IP networks.

The setting is made in the menu Service -> Options on IAdmin Proxy tab.

The proxy IP address and port define the parameters on which the proxy is receiving connections. If the IP address is not specified, then it may be any IP of the server. These parameters are specified in the settings of the client browser to work through IAdmin Proxy. Parameters can be set manually or through group policy in Windows Active Directory or by automatic proxy configuration WPAD server across your internal DHCP and / or DNS server.

The root certificate is required for HTTPS protocols. Admin Proxy does not establish a direct tunnel, and uses the "Trusted man in the middle" technique. The root certificate is a CA certificate on his behalf will be created and signed site certificates.

After the first installation, you must create your own root certificate. Press the corresponding button and enter the name. The certificate name refers to the name of your organization, it will determine the name of the certificate created in Certificates MMC snap-in. The certificate is created under the computer account in the "Trusted Root Certification Authorities."



Export this certificate and store it in a file. Exported certificate must be imported to all client computers, as well in the section "Trusted Root Certification Authorities." This can be done manually (for example, by double clicking on the certificate file from the client computer) or by using the Group Policy of Windows Active Directory ( [https://technet.microsoft.com/en-us/library/Cc731253\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/Cc731253(v=WS.10).aspx) ). Only after import computers are beginning to trust the

Copyright © 2015 Internet Administrator Company Ltd.

<http://www.iadmin.biz>, e-mail: [sales@iadmin.biz](mailto:sales@iadmin.biz)

site certificates, signed with your root certificate, and will not generate an error of invalid certificate. Users will see the name of your company as "Issued" when you open the property of certificate in the browser and when viewing the certificate itself at each site. This title will guarantee the authenticity to users and the security of the connection.

Site certificates are created and stored in the "Personal" section in the Certificates MMC Snap-in on the local computer.

By default Admin Proxy will establish external connections only with websites that have a trusted certificate that contains no errors. If an error occurs, such as an expired certificate, IAdmin Proxy will send to the client browser the corresponding error message. In the setting "Ignore HTTPS server error" you can specify which types of certificate errors will be ignored to establish a connection.

### Section 3.3. - Setting the user login mode

The setting is made in the menu Service -> Options on Modes tab.

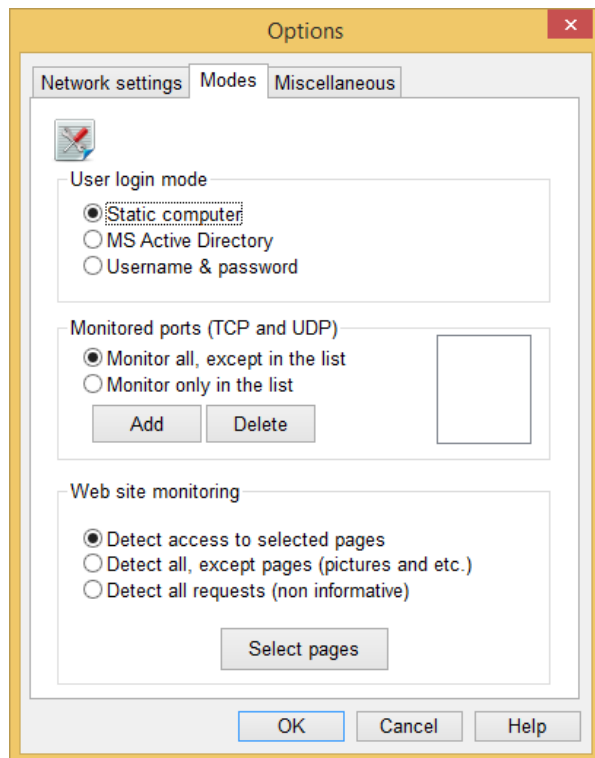
"Internet Administrator" supports three user login types: Static computer, MS Active Directory and Username & password. **Warning! When setting other than Static computer mode, before login process access to the Internet is denied from all computers!** If you have servers and other devices that require internet access without registration, set the checkbox "Set static login at this computer in any modes" in properties of each user that represent such server or device!

In the Static computer mode (by default), user logs in to the workstation on which it was first discovered.

In the Microsoft Active Directory mode user logs in to a workstation after authentication through IAdmin Web with domain account. It uses Integrated Windows Authentication.

Mode by username and password requires entering the registration data for login on the login page of IAdmin Web. Access to the Internet from the workstation will be granted after the user will pass login process.

For more details about IAdmin Web, refer to "4.3 IAdmin Web - statistics and user login"



### Section 3.4. - Custom monitored TCP/UDP ports

The setting is made in the Service -> Options on Modes tab (see screenshot above).

Monitored ports determine which Internet port (Protocol) "Internet Administrator" will monitor. By default all ports are monitored.

Monitored ports are designed primarily to work with a proxy server. Since the proxy server must be excluded from the local IP networks, any requests to it will be considered requests to the Internet. If the proxy server has other network applications, the ports on which these applications run needs to be added to the list as not monitored. If the proxy server provides access to a limited set of ports (HTTP, FTP, POP3, SMTP), they are configured as monitored ports. **Warning! If you set excluded IP addresses, monitored ports will be used only for the excluded addresses.**

### Section 3.5. - Web site monitoring via packet engine

The setting is made in the menu Service -> Options on Modes tab (see screenshot above). This setting determines how program will log requests via HTTP protocol to the database, if IAdmin Proxy is not used.

#### Detect access to selected pages

Requests are recorded to the home page and catalogs of a site, and to selected pages. Pages and files are defined by their extensions, for example, .html, or .zip. To specify the extensions, click «Select pages" and in the window that appears, add or delete the required extension.

#### Detect all, except pages

This mode is set by default. In difference to the previous setting, you specify the page extensions that should not be monitored. This is done in order to ignore image or script requests when the page opens, as they are not of particular interest.

#### Detect all requests

Any request for HTTP protocol is monitored. **This setting is recommended for testing only.** In this mode the main database grows very fast. Also requests to the various scripts and images are not informative in reports and site statistics.

### Section 3.6. - Advanced Settings

The setting is made in the menu Service -> Options on Advanced settings tab.

Database update period. In its work, "Internet Administrator" operates on the data in a operating memory. Periodically, it writes the data into the database. The default value of the update period is 20 seconds. For traceability it can be reduced. It is not recommended to set this parameter is less than 5 seconds. With a large number of users to reduce the load on the processor, this parameter can be increased. Then update the database will occur less frequently.

Time-out of user activity. After the expiration of timeout "Internet Administrator" believes that the user is not active in the internet. Timeout helps to more accurately track the time. The user can open multiple pages and browse them, but there are no new requests from the computer.

Working hours. Set global working hours for separate limits.

Control mode of IP and MAC addresses.

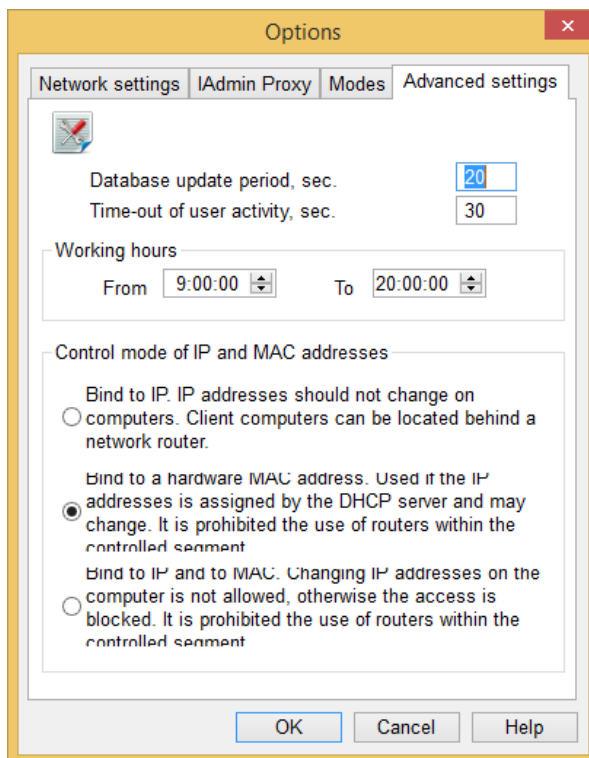
*Bind to IP.* The program monitors computer traffic by IP address only. If existent workstation changes IP address to a new, Internet Administrator finds it as a new computer. This mode is not suitable for use with a DHCP server that changes IP addresses in the same computer.

*Bind to a hardware MAC address.* This is by default. Internet Administrator monitors computers by MAC addresses and found IP changes on workstation automatically.

When you change the IP address on the computer Internet Administrator will making replace the IP in the system. If the changed computer gets an IP address of an existing computer, Internet Administrator will remove IP address from existing computer and set them value as 0.0.0.0, before the discovery of a new IP address on MAC address of existing computer.

**Warning!** Bind to MAC have limitation. Do not use network routers in the internal network because it forwarding packets with the IP addresses of computers and MAC address of router. This does not apply to NAT or proxy servers, as they send traffic from their external IP address.

*Bind to IP and to MAC.* This mode is necessary for protection of IP address changes to set an existing or new address to bypass restrictions. Upon detection of a change of any parameter access will be blocked from IP addresses that do not have the MAC address on a computer registered in the system. This mode has the same router limitation as the previous.

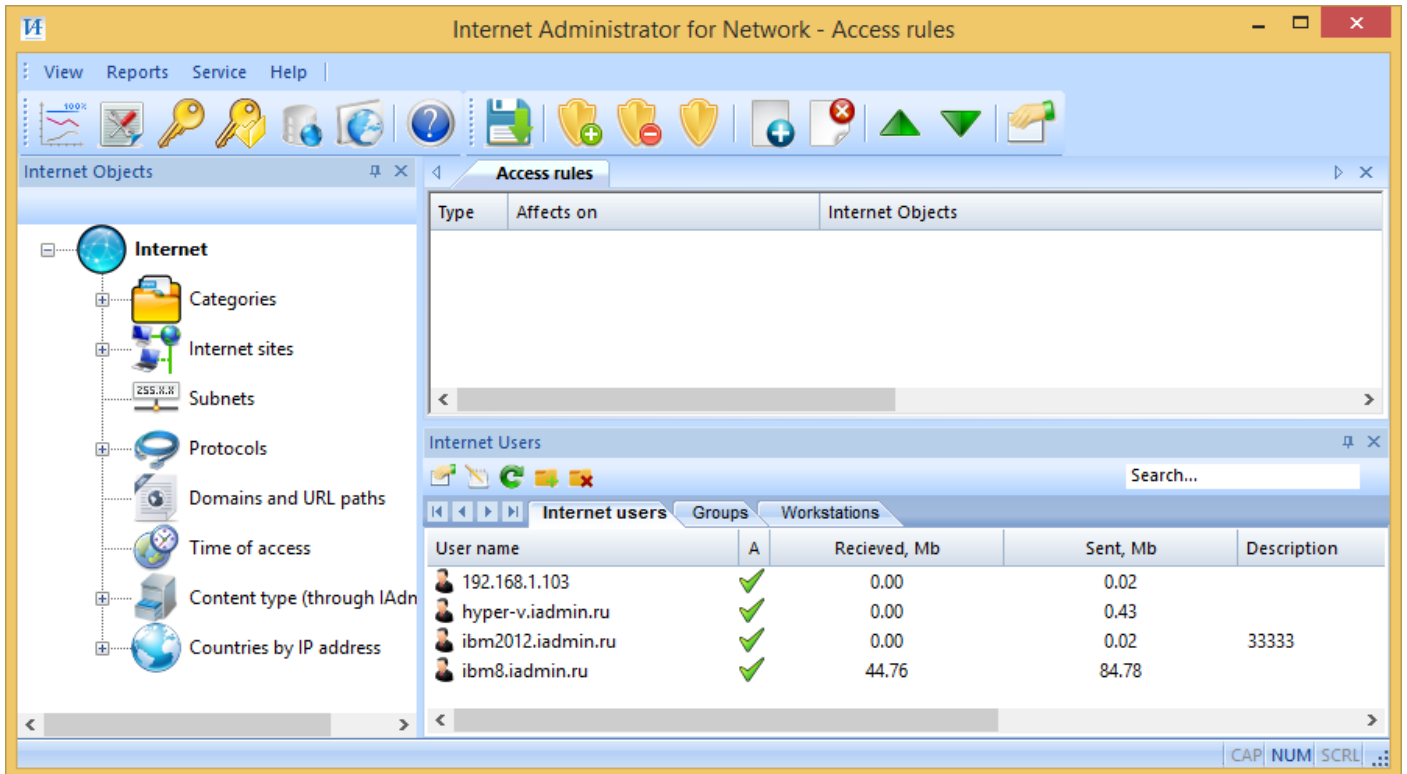



## SECTION 4 - USER MANAGEMENT

This section describes the methods for managing users, groups and computers. All settings in this section are performed from "Rules Admin" utility that located in program group "Internet Administrator".

### Section 4.1. - Users, Groups, and Computers

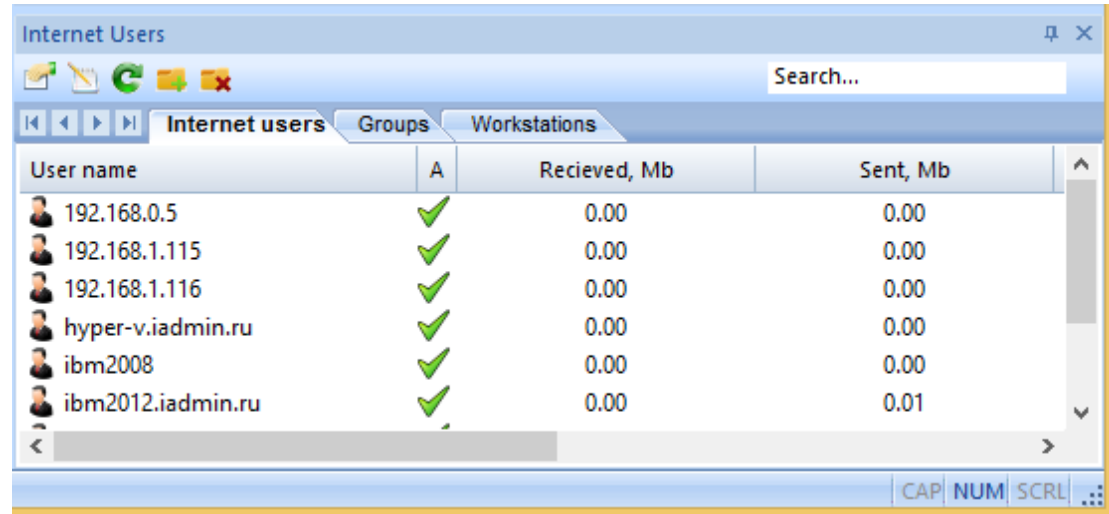
User management is done in the main window of the Rules admin in the lower right area, which is called Internet users.



There are three tabs: Users, Groups, and Workstations. Information in these lists can be updated using a button  on the local toolbar.



## Users



User name	A	Recieved, Mb	Sent, Mb
192.168.0.5	✓	0.00	0.00
192.168.1.115	✓	0.00	0.00
192.168.1.116	✓	0.00	0.00
hyper-v.iadmin.ru	✓	0.00	0.00
ibm2008	✓	0.00	0.00
ibm2012.iadmin.ru	✓	0.00	0.01

The following list is a summary of the user: His name, status of Internet access, how much traffic it is uploaded and sent today and description.

To sort users click on the name of columns. To search user by name type the first letters of the user name in a string "Search..." on the toolbar. A pointer will move to the appropriate user.

By buttons on the toolbar or from right-button menu, you can view  - user properties,  - access log (see Section 6.1) and also  - delete or  - add user.

Deleting of a user will remove the user object and all related information.

Creating a user is only required if you accidentally delete a user in a Static computer mode or in Username and password mode - to create an additional accounts to access the Internet. In any action to create or delete a user, you must restart the service «IAdmin Server».

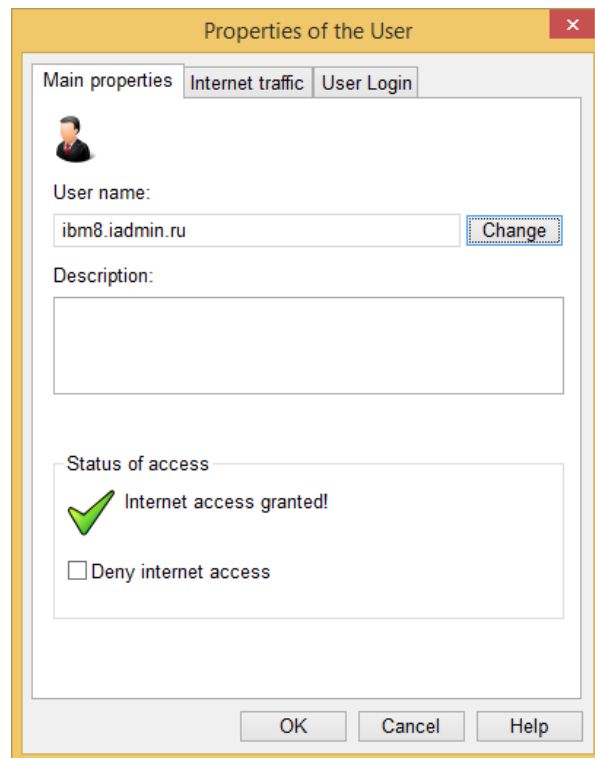
**If you select multiple users, you can set several properties at once the whole list.**

The properties of the user displays three tabs.

On the "Main Properties" you can change the user's full name and its description, as well as manually block the user - in this case access to the Internet will be denied by force.

Changing the system name can be made for natural display in reports. System Name - the name of the user defined by the system when it detects the workstation. This can be a domain name, host name, or IP address. In MS Active Directory mode names cannot be changed, because in this mode they are the domain names registered by the system.

If a user is blocked by the system, before unblocking, you must first increase the available limits; otherwise it will be blocked again.



The screenshot shows the 'Properties of the User' dialog box with the 'Main properties' tab selected. It features a user icon, a 'User name' field with the value 'ibm8.iadmin.ru' and a 'Change' button, a 'Description' text area, and a 'Status of access' section with a green checkmark and the text 'Internet access granted!'. There is also an unchecked checkbox for 'Deny internet access'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

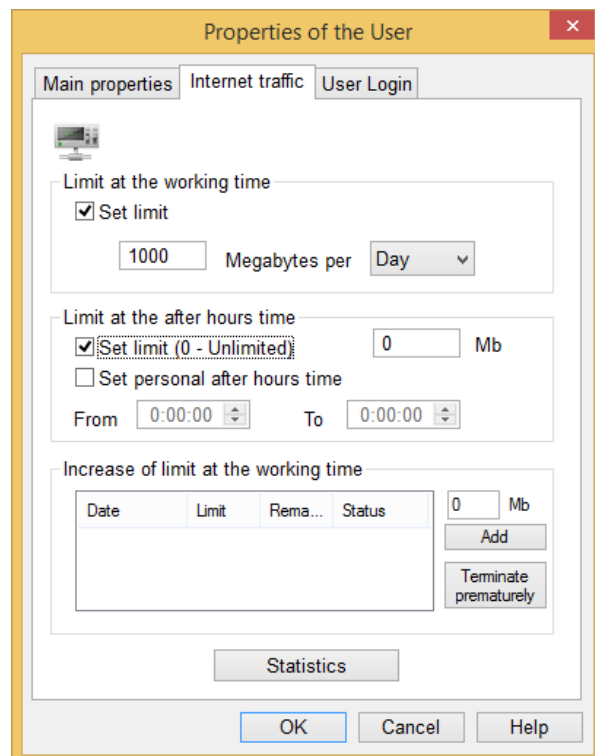
On the "Internet Traffic" tab are defined user traffic limits by volume.

To limit incoming traffic, enable appropriate mode and set the limit data and the accounting period. If you set limit at the working time only it will work the whole day.

Accounting period - the time during which a limit will work. After threshold the user will be blocked. Traffic limit is specified in megabytes.

You can specify a separate limit for the afterhours time of day. If you specify 0, the traffic at the afterhours time will be unlimited.

In the case of the threshold in the working time, you can add to it a few more megabytes of traffic for current accounting period. To do this, use "Increase of limit in the base time" section.



The screenshot shows the 'Properties of the User' dialog box with the 'Internet traffic' tab selected. It contains sections for 'Limit at the working time' (with a checked 'Set limit' box, a value of '1000', and a unit of 'Megabytes per Day'), 'Limit at the after hours time' (with a checked 'Set limit (0 - Unlimited)' box, a value of '0', and a unit of 'Mb'), and 'Set personal after hours time' (unchecked). There are also time pickers for 'From' and 'To' both set to '0:00:00'. A table titled 'Increase of limit at the working time' has columns for 'Date', 'Limit', 'Rema...', and 'Status'. To the right of the table are 'Add' and 'Terminate prematurely' buttons. A 'Statistics' button is at the bottom. At the very bottom are 'OK', 'Cancel', and 'Help' buttons.

User Login tab displays the current user login and is intended to set the user name and password to login with the appropriate mode.

User login can be manually changed. It is necessary if you accidentally delete the user and re-creating it, or when switching from other login modes to Static computer mode.

Use the check box "Set static login in any modes" for servers and devices running without the user to use Static computer mode, otherwise Internet access will be blocked without login process!

Properties of the User

Main properties Internet traffic User Login

Current login data

Computer: ibm8.iadmin.ru

IP address: 192.168.1.15

Set static login in any modes ☐

Login by name and password

Username:

Password:

Repeat

Change login computer

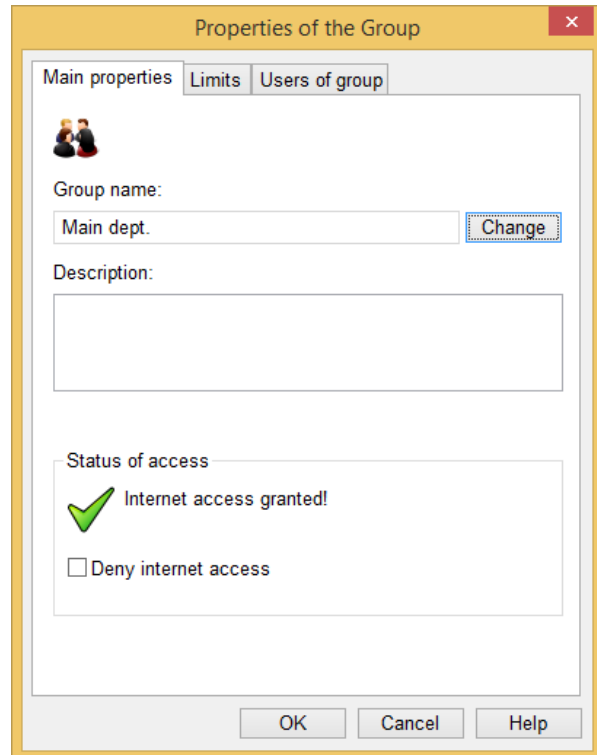
OK Cancel Help

## User groups

A group contains users. Any actions with a group apply to all users in it. From the toolbar or the context mouse menu you can open the property of group (📄), create (➕), or delete (✖) the group. The group name must be unique. By default, there is a "System" group, which includes users who are not members of other groups. "System" group cannot be renamed or deleted.

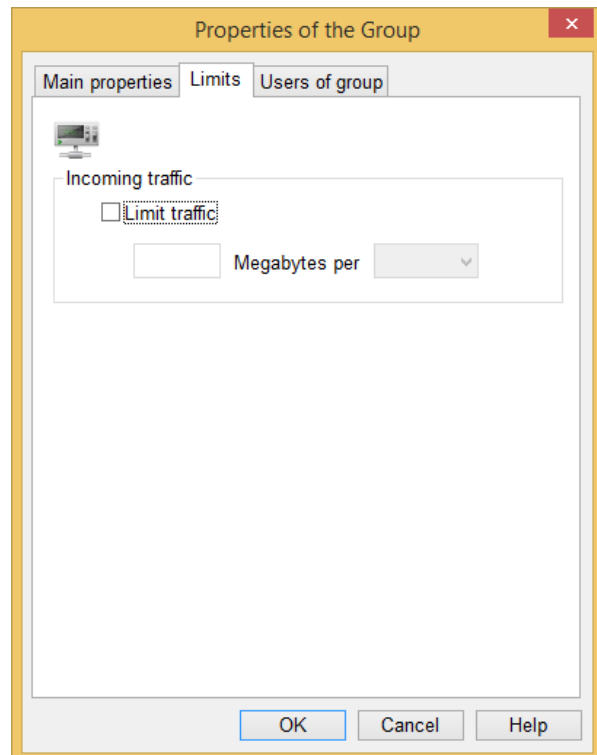
The group properties display three tabs.

"Main properties" displays the name of the group and description. On this tab, you can deny internet access to all users of the group.



The screenshot shows the 'Properties of the Group' dialog box with the 'Main properties' tab selected. It features a group icon, a 'Group name' field with 'Main dept.' and a 'Change' button, a 'Description' text area, and a 'Status of access' section with a checked 'Internet access granted!' option and an unchecked 'Deny internet access' option. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

"Limits" tab sets limit on incoming traffic from the Internet to all members of the group. When the limit is reached, the group and all users in it will be blocked.

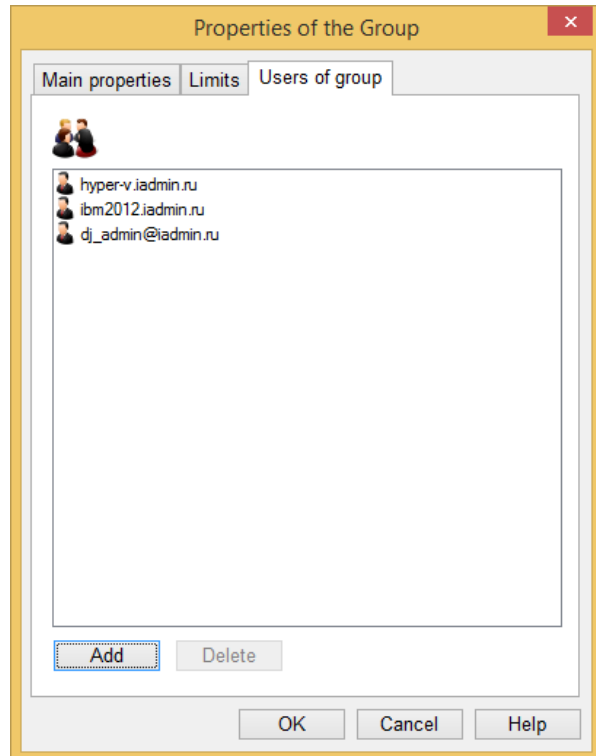


The screenshot shows the 'Properties of the Group' dialog box with the 'Limits' tab selected. It features a computer icon, an 'Incoming traffic' section with an unchecked 'Limit traffic' checkbox, and a field for 'Megabytes per' with a dropdown arrow. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

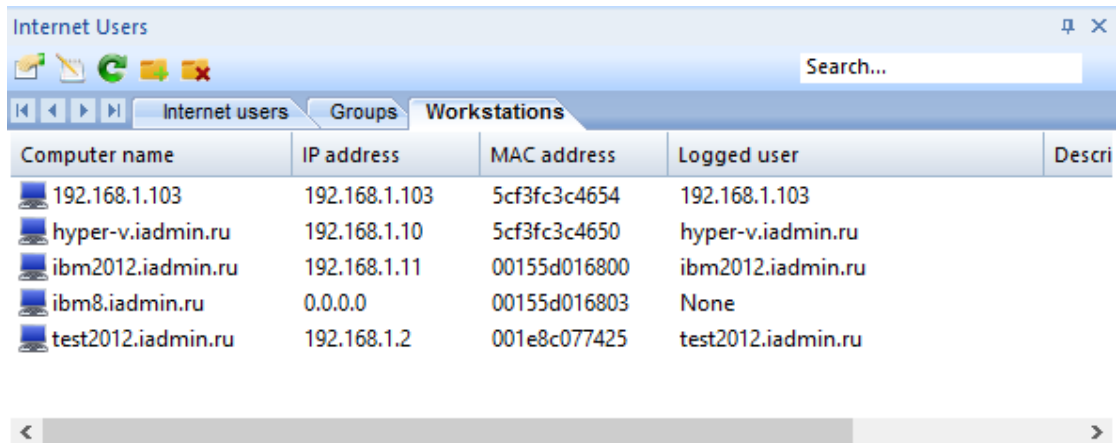
The "Users" tab displays a list of group members.

From here you can add or delete users. When you add a user it is removed from the previous group membership. When you delete it becomes a member of the "System" group. The user can not be a member of two or more groups, it can only move between the existing groups.

By default, all users when it detects fall into the System group. Use it if you want to automatically block all new users. To do this, move users to other groups and block the System group. Now all new users will have no access to the Internet till you add it to a custom group.




## Workstations (computers)




Computer name	IP address	MAC address	Logged user	Descri
192.168.1.103	192.168.1.103	5cf3fc3c4654	192.168.1.103	
hyper-v.iadmin.ru	192.168.1.10	5cf3fc3c4650	hyper-v.iadmin.ru	
ibm2012.iadmin.ru	192.168.1.11	00155d016800	ibm2012.iadmin.ru	
ibm8.iadmin.ru	0.0.0.0	00155d016803	None	
test2012.iadmin.ru	192.168.1.2	001e8c077425	test2012.iadmin.ru	

This list shows all detected workstations on your network. It provides information about the name of the workstation and its IP and MAC addresses, as well as the user who is currently logged on. Workstation can be transferred to the list of unmonitored workstations for which requests are not served. , delete or open its properties. In the properties of a workstation, you can write to her description, as well as change its credentials such as name, IP address and MAC address.

## Section 4.2. - Internet access log


Access log is available in the main window in the section of Internet users. Choose a user, and then in the context menu or button , open it.

Access log						
<div>  <div>Time period and page filter</div> <div> <div>05.06.2015</div> <div>—</div> <div>05.06.2015</div> </div> <div> <input checked="" type="radio"/> View sites only  <input type="radio"/> View sites and pages         </div> </div>						
Host	Hits	Category	Last time of access	Recv, Kb	Sent, Kb	
www.sunsy-online.com	5	None	05.06.2015 18:16:21	5201,00	233,68	
www.telize.com	2	None	05.06.2015 17:47:44	91,18	24,13	
www.tns-counter.ru	289	None	05.06.2015 19:11:07	528,00	175,76	
www.topmagic.org	2	None	05.06.2015 18:12:40	173,97	14,25	
www.twhvolleyball.com	2	None	05.06.2015 18:13:22	12,68	1,49	
www.under-top.org	2	None	05.06.2015 18:14:07	54,58	6,10	
www.vacheries.fr	1	None	05.06.2015 18:14:06	87,48	4,30	
www.vitorrent.me	1	None	05.06.2015 18:15:08	68,07	7,77	
www.wikidata.org	6	None	05.06.2015 16:55:57	32,18	6,38	
www.yandex.ru	22	Search Engines;	05.06.2015 19:00:20	259,41	23,91	
www.youtube.com	18	Streaming Media/MP3;	05.06.2015 18:23:27	4650,83	246,76	
www.zecurion.ru	3	None	05.06.2015 13:33:26	173,12	24,75	
www1.adnkronos.com	3	None	05.06.2015 16:29:52	3,33	3,35	
www3.l.gle.com	18	None	05.06.2015 18:23:16	6,53	12,14	
www-da1.adobe.com	4	None	05.06.2015 18:14:25	0,26	0,47	
www-google-analytics.l.google.	101	None	05.06.2015 19:11:07	321,97	70,87	
www-googletagmanager.l.google.	6	None	05.06.2015 16:32:11	0,32	0,65	
www-hc-573304892.eu-west-1....	14	None	05.06.2015 19:02:37	0,90	1,64	
www-wide.i.l.google.	11	None	05.06.2015 18:23:15	2,64	3,11	
v.birdswitch.net	6	None	05.06.2015 17:50:47	16,98	4,65	

Access log shows the websites and hosts visited. Above the window date filter and two viewing modes are located.

"View sites only" displays summary information about the visits - the site name, the number of requests, category, date of last access, and the amount of downloaded and uploaded data. In the context menu you can set the site category, if it is not set, and open it in the browser for analysis.

“View sites and pages” displays more detailed information in chronological order.

Access log							
<div>  <div>Time period and page filter</div> <div> <div>05.06.2015</div> <div>—</div> <div>05.06.2015</div> </div> <div> <input type="radio"/> View sites only  <input checked="" type="radio"/> View sites and pages                 </div> </div>							
Host	Action	Category	Protocol	Time of access	Resv, Kb	Sent, Kb	
csi.gstatic.com	/	None	HTTPS	05.06.2015 20:02:51	0,06	0,12	
google.ru	/	Search Engines;	HTTPS	05.06.2015 20:02:51	0,06	0,12	
google.ru	/	Search Engines;	HTTPS	05.06.2015 20:02:51	0,06	0,12	
csi.gstatic.com	/	None	HTTPS	05.06.2015 20:02:51	0,06	0,12	
224.0.0.252	/	None	5355	05.06.2015 19:59:06	0,00	0,13	
csi.gstatic.com	/	None	HTTPS	05.06.2015 19:58:44	0,06	0,12	
csi.gstatic.com	/	None	HTTPS	05.06.2015 19:58:44	0,06	0,12	
csi.gstatic.com	/	None	HTTPS	05.06.2015 19:58:44	0,76	1,40	
csi.gstatic.com	/	None	HTTPS	05.06.2015 19:58:44	0,39	0,75	
239.255.255.250	/	None	1900	05.06.2015 19:58:44	0,00	9,11	
translate.google.ru	/	None	HTTPS	05.06.2015 19:58:43	4,12	7,28	
google.ru	/	Search Engines;	HTTPS	05.06.2015 19:58:43	0,06	0,12	
translate.google.ru	/	None	HTTPS	05.06.2015 19:58:42	2,06	12,69	
google.ru	/	Search Engines;	HTTPS	05.06.2015 19:58:42	0,06	0,12	
google.ru	/	Search Engines;	HTTPS	05.06.2015 19:58:42	0,06	0,12	
translate.google.ru	/	None	HTTPS	05.06.2015 19:58:42	0,44	0,80	
DEPO	/	None	NetBios ...	05.06.2015 19:57:36	1,76	1,64	
csi.gstatic.com	/	None	HTTPS	05.06.2015 19:57:20	0,06	0,12	
csi.gstatic.com	/	None	HTTPS	05.06.2015 19:57:20	0,39	0,75	
csi.gstatic.com	/	None	HTTPS	05.06.2015 19:57:20	0,76	1,40	

Here we can see requests as they are visited by the user. In addition to the sites themselves, service requests that the user does not perform are logged here, but they are part of the site, so the browser opens its together. If access to the site was blocked, it is highlighted in red. For more information, use the reports (Section 7).



### Section 4.3. – IAdmin Web - statistics and user login

To set up a web server see Section 3.1. Web server implements two functions: display statistics and login a user.

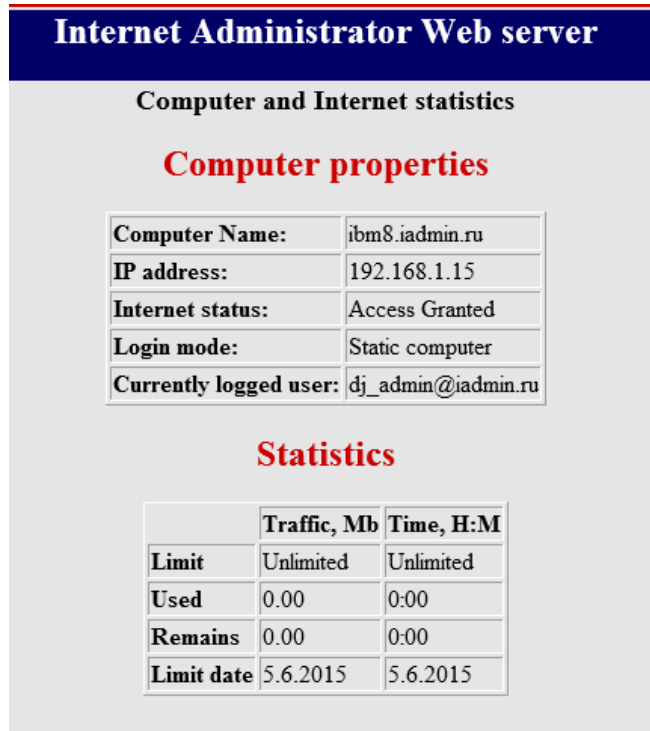
Connection to the Web server should be implemented from client computers. To access the Web server use the IP address or the name of the server that is running Internet Administrator, as well as the port specified in the configuration (8008 by default). The address looks like this <http://192.168.1.1:8008/>

#### Display statistics

When you open a Web server it gives statistics of the computer from which the connection was made.

Here you can see the computer data, such as name and IP address. Status indicates whether there is blocking access.

Statistics show data limits, if they are given, and the current balance, similar to the data in the user properties.



The screenshot displays the 'Internet Administrator Web server' interface. At the top, a blue header bar contains the title 'Internet Administrator Web server'. Below this, the section 'Computer and Internet statistics' is shown. Underneath, the heading 'Computer properties' is displayed in red. A table lists the following information: Computer Name (ibm8.iadmin.ru), IP address (192.168.1.15), Internet status (Access Granted), Login mode (Static computer), and Currently logged user (dj\_admin@iadmin.ru). Below this table, the heading 'Statistics' is shown in red. A second table provides data on traffic and time limits: Limit (Unlimited), Used (0.00), Remains (0.00), and Limit date (5.6.2015).

	Traffic, Mb	Time, H:M
Limit	Unlimited	Unlimited
Used	0.00	0:00
Remains	0.00	0:00
Limit date	5.6.2015	5.6.2015

#### Login a user

To access the Internet in MS Active Directory and Name & password login modes, the user must complete the login process by accessing the Web server from workstation. Prior to the login, an access to the Internet is blocked and all requests for HTTP protocol will be redirected automatically to the Web server.

To logoff, the user must open the Web server logoff page (for example, <http://192.168.1.1:8008/logoff>), or press the Logoff link that appears after the user name on the statistics page. To automate this process use domain group policy to access logoff page when the user logged of from a domain.

**If a user does not make logoff through the Web server, the next user will be working on behalf of the previous one, and Internet Administrator will not prompt for new registration request.**

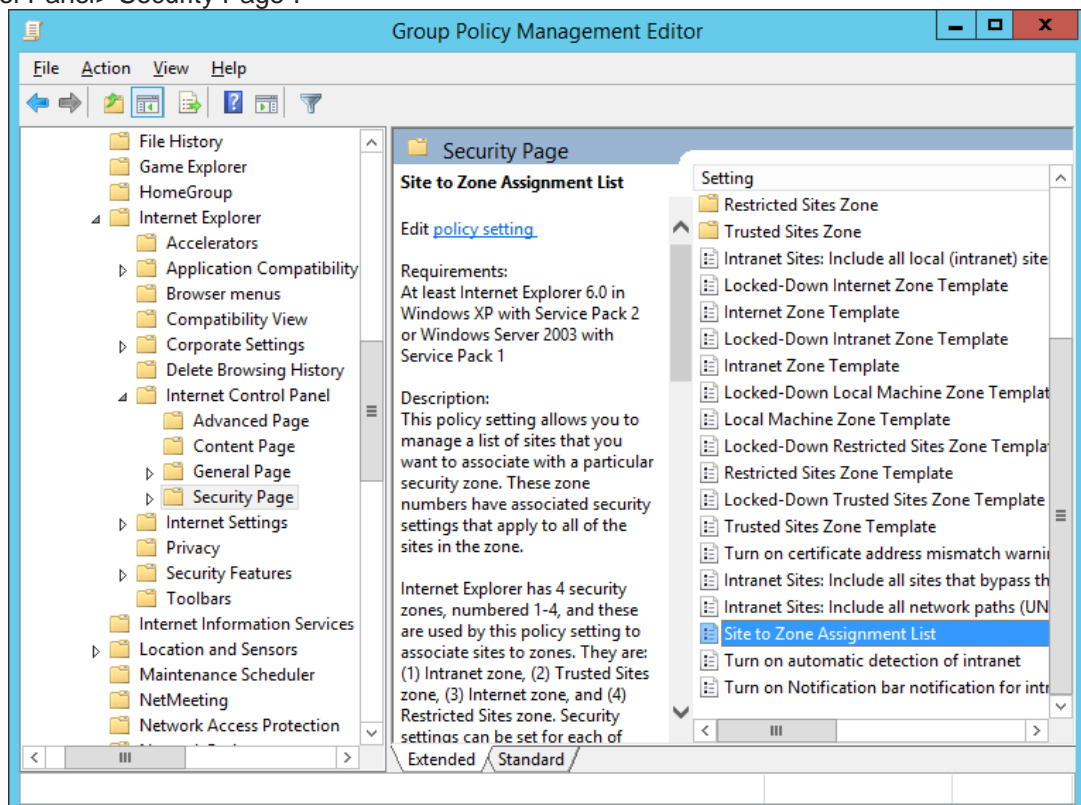
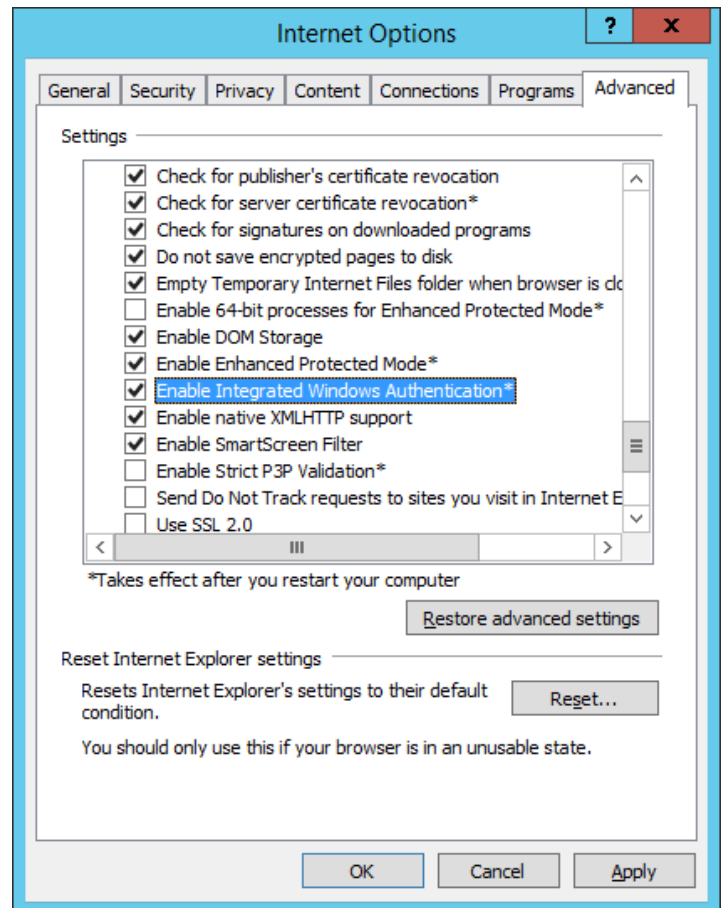
### MS Active Directory login

If mode set to MS Active Directory, Web server attempts to obtain data about domain user name. It uses the integrated Windows authentication, which is supported in all modern browsers. Make sure that integrated authentication is enabled in browsers on workstations (it's enabled by default). See Internet Explorer properties to check authentication below.

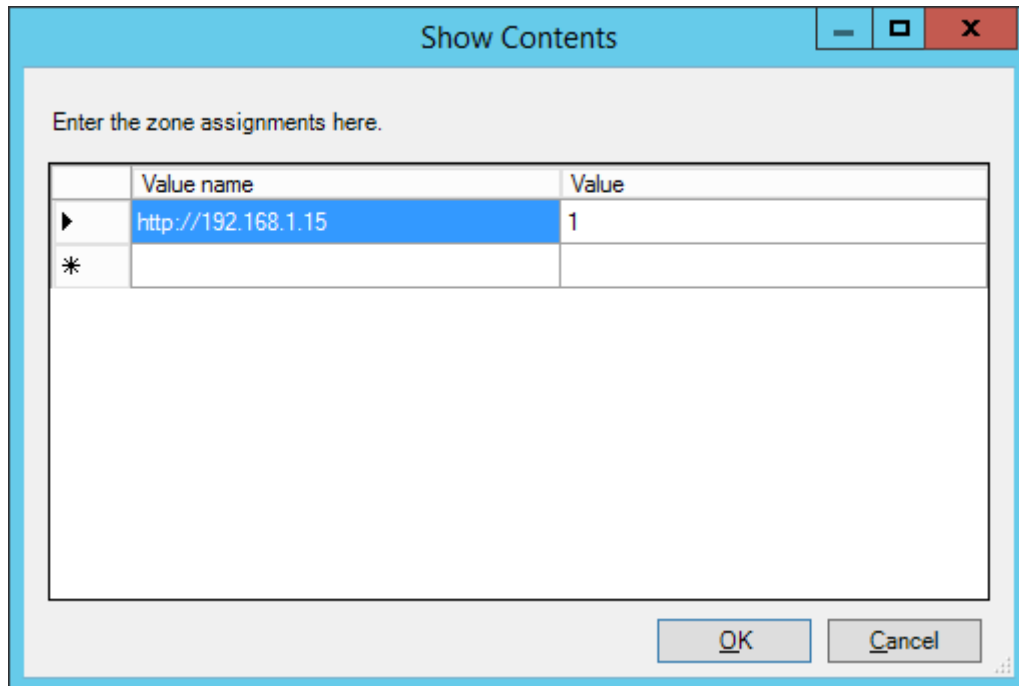
The authentication process involves three computers: a user workstation, Internet Administrator server and Active Directory domain controller. A controller certifies that a user is logged into domain and sends its security descriptor, from which IAdmin Web receives the user name for the login process.

If automatic authentication is disabled, the browser will request the domain name and password. These names and passwords are not transferred to IAdmin Web. User authentication is processed by domain controller, and only after receiving a domain data, IAdmin Web will be able to login a user!

**To enable automatic authentication** that the user did not enter domain name and password, add the address of IAdmin Web to the security zone "Local intranet" on each computer. This can be done centrally through domain group policy. Setting path is "Computer Configuration> Administrative Templates> Windows Components> Internet Explorer> Internet Control Panel> Security Page".



Add to «Site to Zone assignment list» URL of the IAdmin Web server by which it is accessed and set the network type 1.



The 'Show Contents' dialog box has a title bar with standard window controls. Inside, it says 'Enter the zone assignments here.' Below this is a table with two columns: 'Value name' and 'Value'. The first row has a right-pointing triangle icon in the 'Value name' column, followed by 'http://192.168.1.15' and '1' in the 'Value' column. The second row has an asterisk icon in the 'Value name' column and is empty in the 'Value' column. At the bottom right are 'OK' and 'Cancel' buttons.

	Value name	Value
▶	http://192.168.1.15	1
*		

### Name&Password login

In Name&Password mode Web Server will ask user to enter login data at the bottom of the main page.

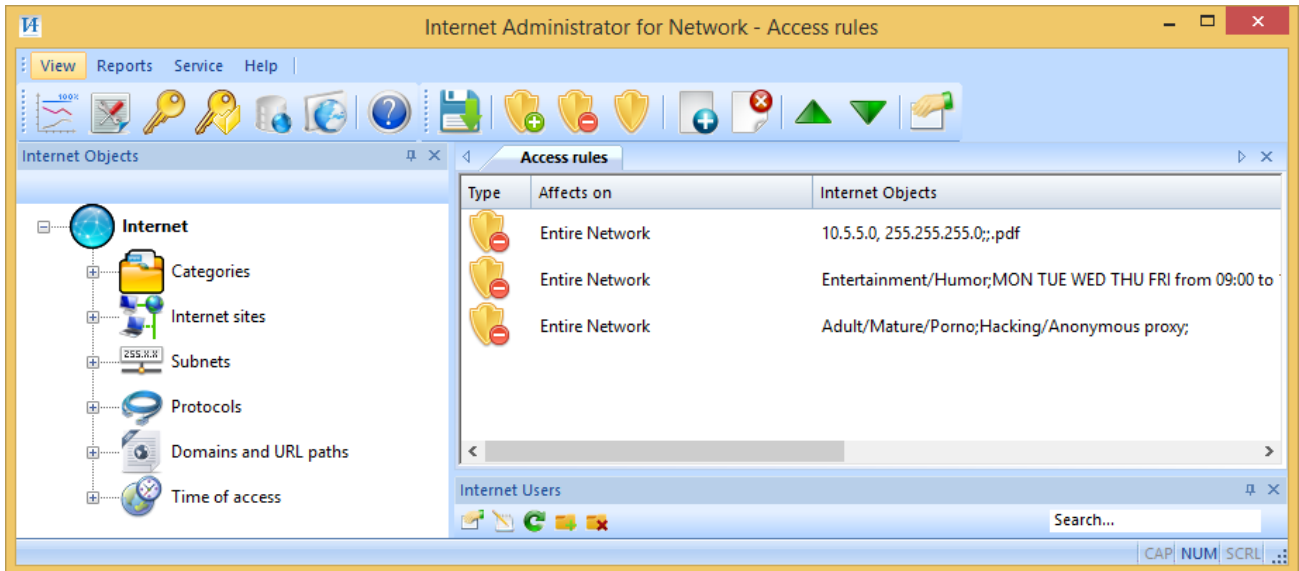


The login form has a title 'User name and password' in red. Below it is the instruction 'Please authorize to access the Internet'. There are two input fields: 'Username:' and 'Password:'. At the bottom are 'Login' and 'Clear' buttons.

This user name and password must be set by administrator in User properties before it can log in.

## SECTION 5 - INTERNET ACCESS CONTROL

This section describes the methods to manage Internet. The main window of "Rules Administrator" displays a list of access rules, the Internet object tree, as well as a list of Internet users.




### Section 5.1. - A set of rules

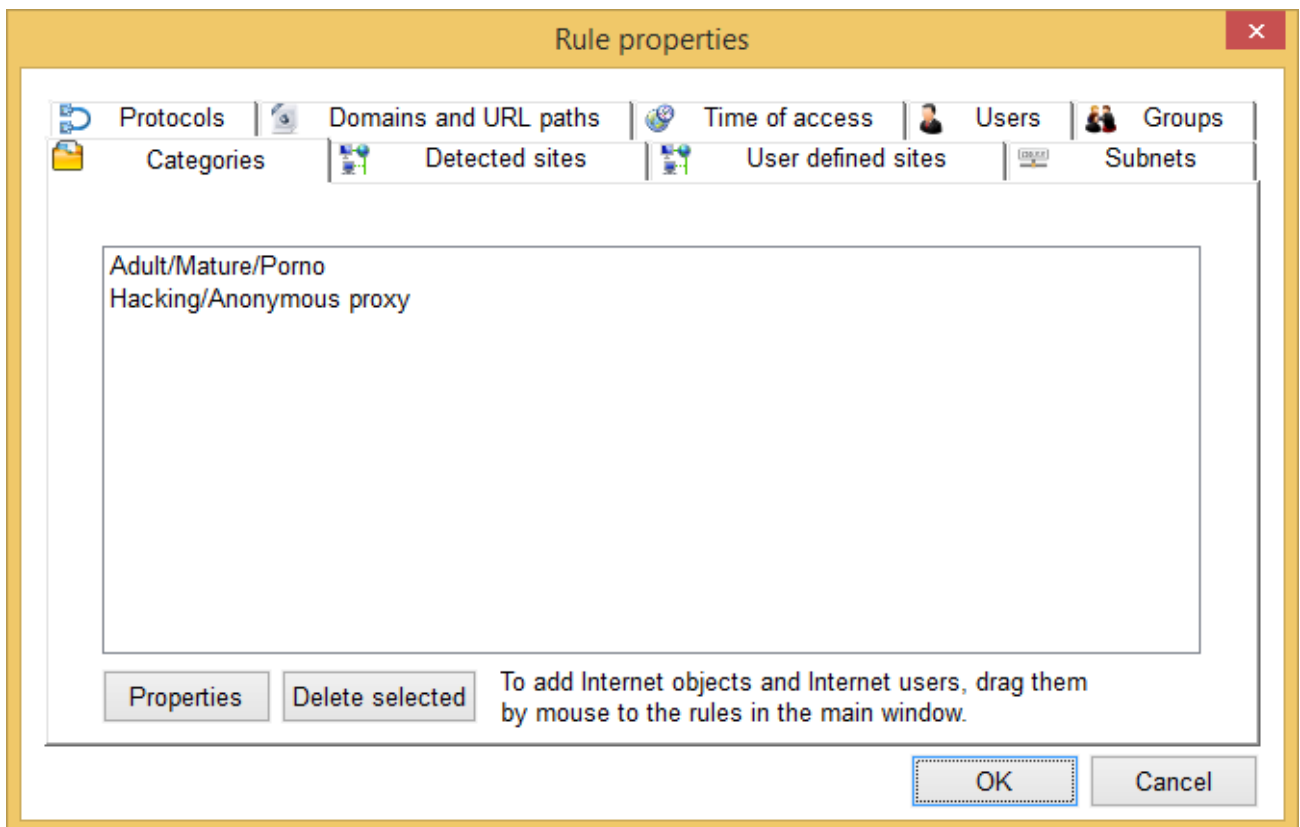
A set of rules determines the access policy - who, when, where and how can access to the Internet.

The rules work from the top to down by priority, the highest priority has the latest on the list. A rule can allow or deny access and to be turned off while it is not taken into account in the overall access policy. If no any rule access is not limited.

A rule can be created from the context menu, or drag and drop any object on the free rule space. New rule allows access to all resources for all.

Addition of objects to a rule is done by mouse drag and drop to the desired rule or on a free area in the rules. **To accept changes you need to click save button**  **in main tool bar.**

In the menu or double-clicking the rule it opens its properties.



Here you can view and delete objects and Internet users that were previously added to the rule, as well as properties.

## Section 5.2. - How do the rules

Rules work through the list from top to bottom. Lower rule has priority over the higher, and may cancel or reinforce them. The system searches first deny rule and the objects in it, and then searches permitting rule down the list. If permitting rule is not found, access will be blocked. If an allow rule is found, system searches deny rule down the list again and so on.

### Пример.

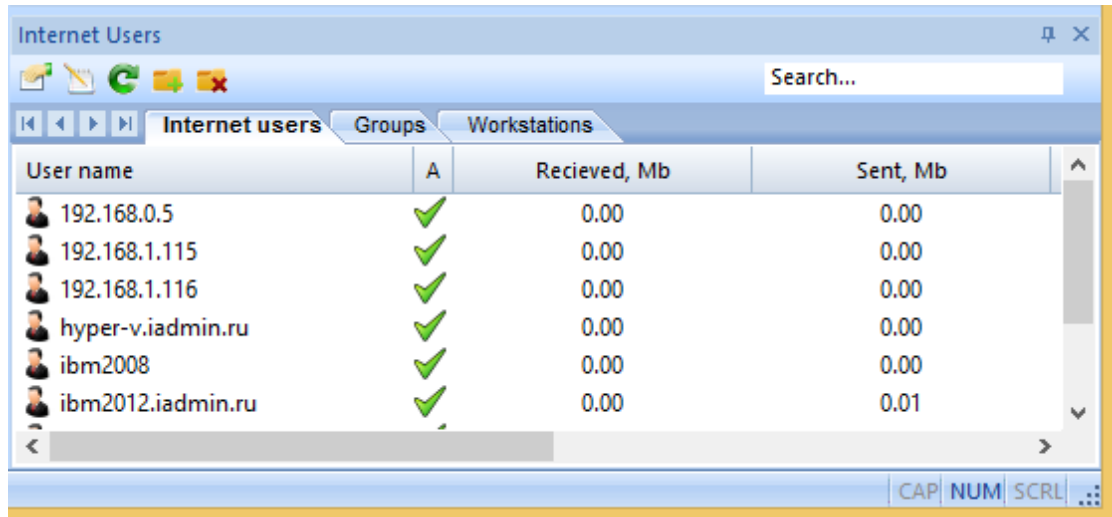
Access rules		
Type	Affects on	Internet Objects
	Entire Network	Adult/Mature/Porno;Hacking/Anonymous proxy;
	Entire Network	Entertainment/Humor;
	Entire Network	Entertainment/Humor;MON TUE WED THU FRI from 13:00 to 14:00

The first two rules in the above figure is blocking access to the appropriate categories. However, the third rule makes an exception and allows access to entertainment sites during lunch time from 13 to 14 hours. However, if there were a fourth rule that blocks access to a particular site of the Entertainment category, this site would be unavailable at any time, regardless of the third rule.

### Section 5.3. - Elements of the rule

#### Users and Groups

Users and groups - this is the first type of elements that defines who is affected by a rule. If users and groups are not included in a rule, it applies to the whole network.



The screenshot shows the 'Internet Users' window with a search bar and tabs for 'Internet users', 'Groups', and 'Workstations'. The 'Internet users' tab is active, displaying a table with columns: 'User name', 'A', 'Recieved, Mb', and 'Sent, Mb'.

User name	A	Recieved, Mb	Sent, Mb
192.168.0.5	✓	0.00	0.00
192.168.1.115	✓	0.00	0.00
192.168.1.116	✓	0.00	0.00
hyper-v.iadmin.ru	✓	0.00	0.00
ibm2008	✓	0.00	0.00
ibm2012.iadmin.ru	✓	0.00	0.01

At the bottom right of the window, there are buttons for 'CAP', 'NUM', and 'SCRL'.

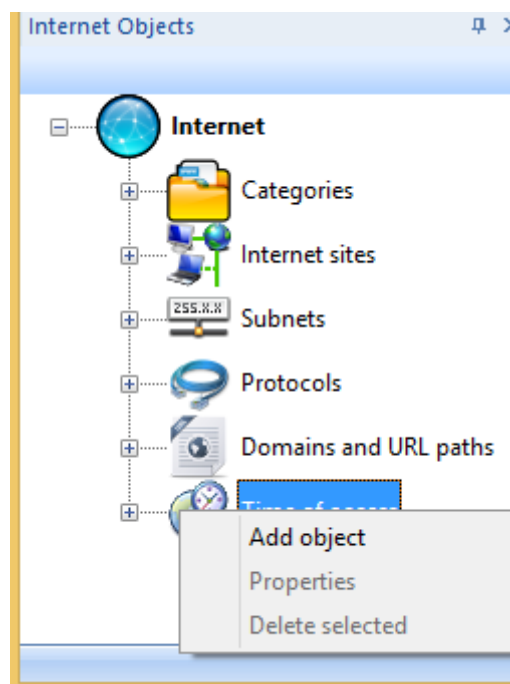
#### Internet objects

Internet objects is the second type of elements that defines to what a rule will block or allow. If one rule defined several different Internet objects, its action will be defined jointly when deciding to restrict access. For example, if one rule is blocked by a particular site and time, than access to this site will be blocked only at a specified time.

Together in a single rule can be combined two groups:

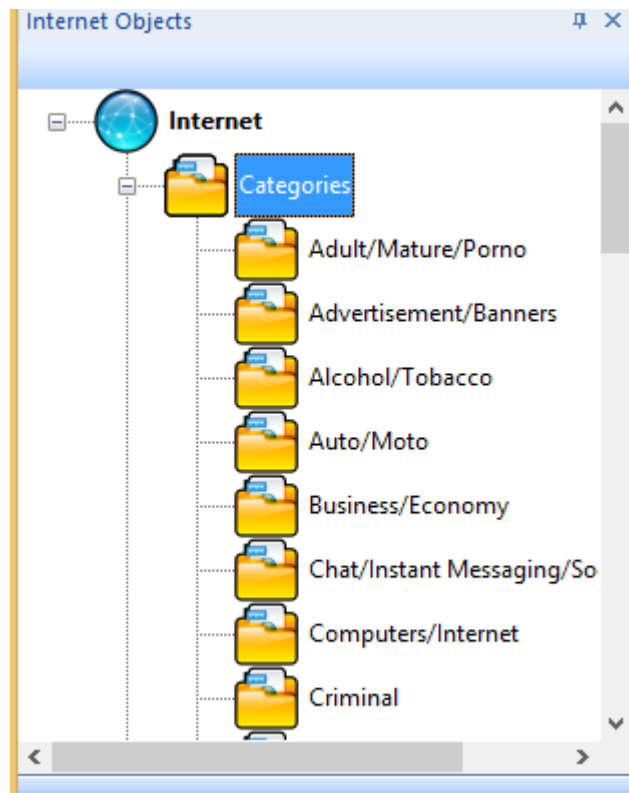
- Sites, subnets, protocols, domains and URL paths, and time of access;
- Categories and time of access.

To add internet objects to the appropriate list, use the context mouse menu.



In this menu you can also view the properties of the object and remove it when the menu is opened directly with the selected object.

### Internet Administrator URL Category database



The list contains 38 standard categories with more than 4 million sites. Using categories is available only after you enter the Category database license key and linking it to the current server. See Section 6.2. - Licensing category database for more information.

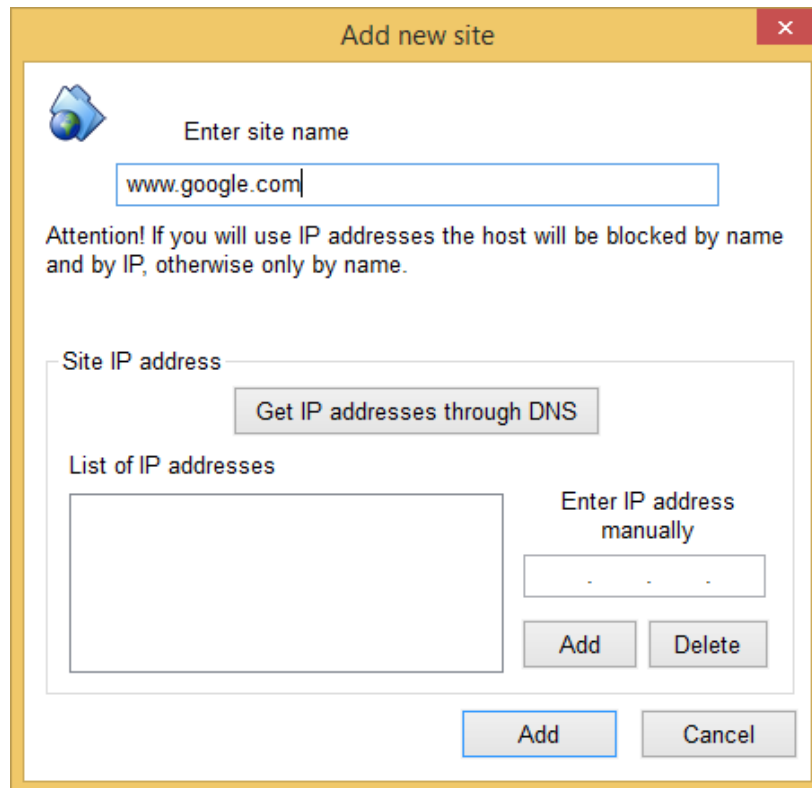
Description of the standard categories can be found here <http://www.iadmin.biz/products/?pid=7>.

It is not possible to see or edit sites included in the standard categories. To test a site you can use our service <http://www.iadmin.biz/support/urlchecker/>.

In addition to the standard categories provided for the addition of custom categories. In these categories the administrator himself adds the necessary sites.

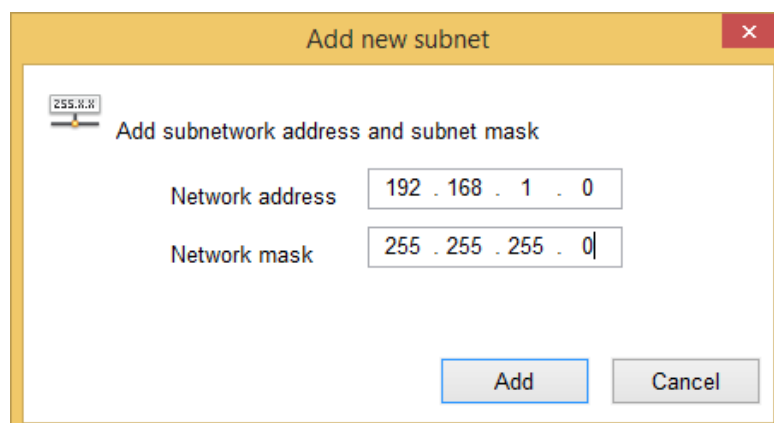
## Internet sites (Hosts)

Sites presented two lists - detected and user defined. Detected sites are found in the user queries, these are the sites that have ever been accessed. User defined sites are added manually by the administrator.



Site can be added with name and IP address. IP address is an optional parameter. If it is not specified, the rule will process only HTTP protocol and web site name, otherwise access will be checked by IP addresses of the host on any protocol also. The address can be obtained by using the name resolution mechanism. To do this, click "Get IP addresses through DNS".

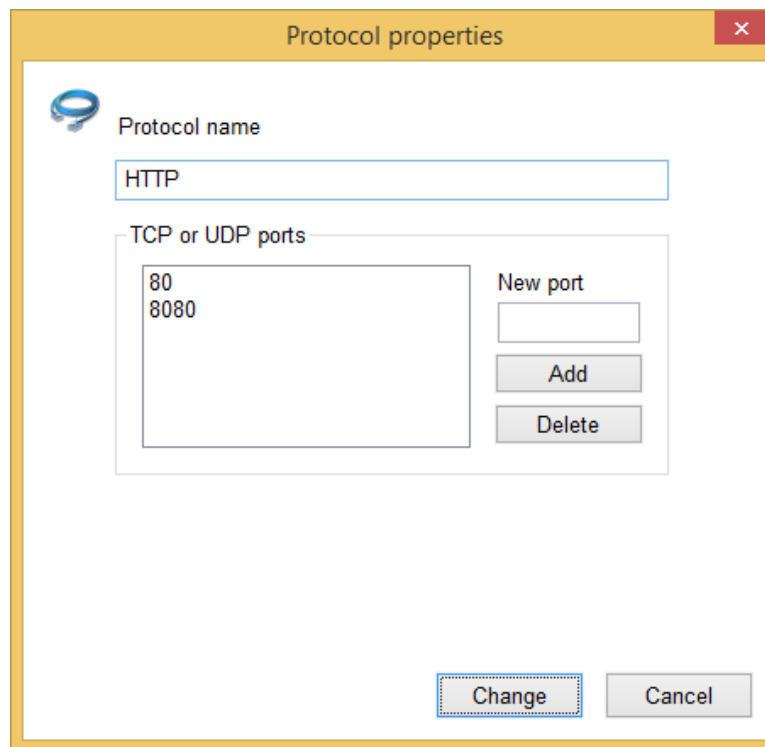
## Subnets



This object defines a set of Internet hosts by IP address. The addresses are given in the form of IP-based network addresses and masks.



## Internet protocols



The image shows a 'Protocol properties' dialog box with a yellow title bar and a red close button. Inside, there is a blue icon of a network cable. The 'Protocol name' field contains 'HTTP'. Below it, the 'TCP or UDP ports' section contains a list box with '80' and '8080'. To the right of the list box is a 'New port' input field, and below it are 'Add' and 'Delete' buttons. At the bottom of the dialog are 'Change' and 'Cancel' buttons.

Protocol properties

Protocol name

HTTP

TCP or UDP ports

80  
8080

New port

Add

Delete

Change

Cancel

Protocols contain a list of TCP/UDP ports, in which data is transmitted between a workstation and Internet hosts. By default, this object contains a list of standard protocols.

## Domains and URL paths

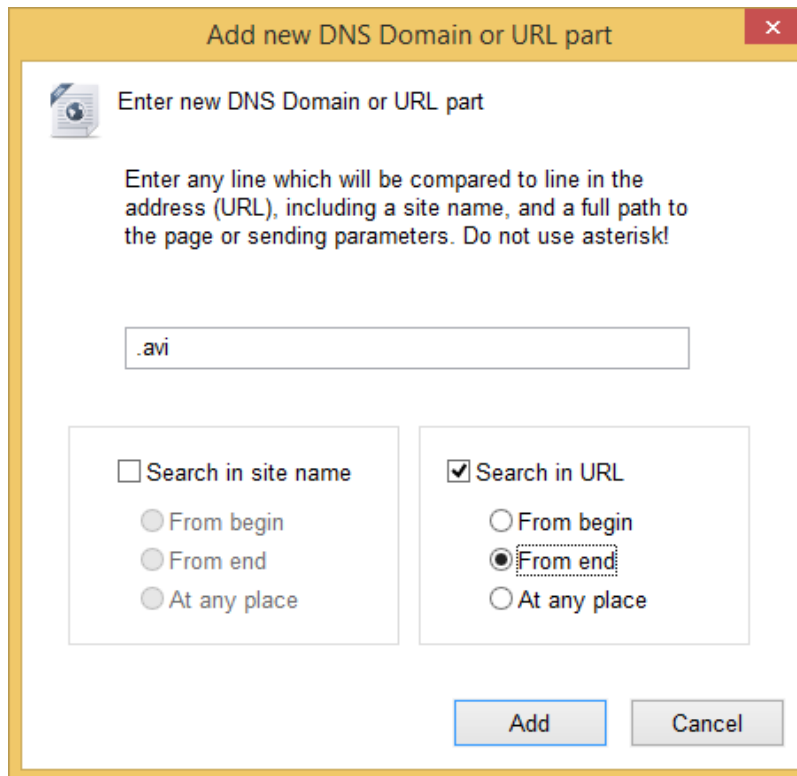
Domains and URL paths is an object to search strings that will be compared with the site name and/or URL of the request. URL paths work over HTTP only.

For example, look at this request (address) <http://abc.com:80/~smith/home.html>. Here abc.com is a site name and ~smith/home.html is a URL path (abs\_path).

So you can search in sites this way:

- Enter "ab" string and set "From begin" will make rule to action on any site starting from ab, for example abc, abd, abe.
- Enter ".com" string and set "From end" will make rule to action on any site in .com root domain.
- Enter "abc" string and set "At any place" will make rule to action on any site having this string in name everywhere.

Search in URL is similar above.



**Add new DNS Domain or URL part**

Enter new DNS Domain or URL part

Enter any line which will be compared to line in the address (URL), including a site name, and a full path to the page or sending parameters. Do not use asterisk!

☐ Search in site name

☐ From begin

☐ From end

☐ At any place

☒ Search in URL

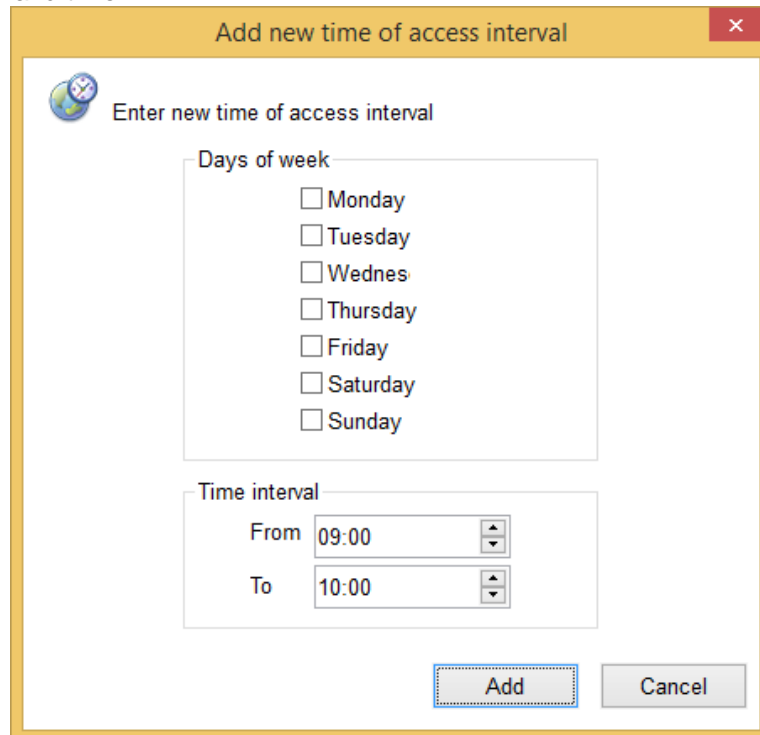
☐ From begin

☒ From end

☐ At any place

## Time of access

This object specifies the time interval in which the rules will action. The time of access is a set of days of week and time.



**Add new time of access interval**

Enter new time of access interval

**Days of week**

☐ Monday  
☐ Tuesday  
☐ Wednesday  
☐ Thursday  
☐ Friday  
☐ Saturday  
☐ Sunday

**Time interval**

From: 09:00  
To: 10:00

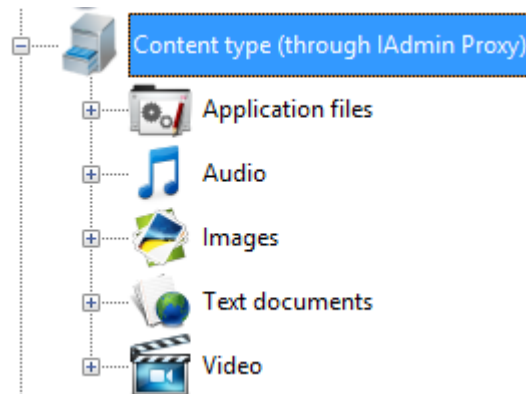
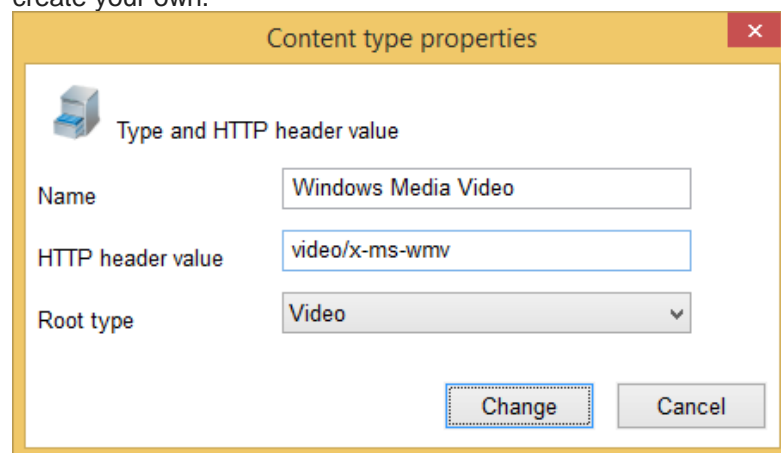
**Add** **Cancel**

## Content type

**Attention! Content type objects will work only for computers configured to use Admin Proxy as HTTP/HTTPS proxy server.**

Type of content indicates the type of response the web server. Here are application files, audio and video content, images, web pages as well as text documents. The content type is determined in accordance with MIME types for HTTP header Content-Type.

You can edit the default types or create your own.

**Content type properties**

Type and HTTP header value

Name: Windows Media Video

HTTP header value: video/x-ms-wmv

Root type: Video

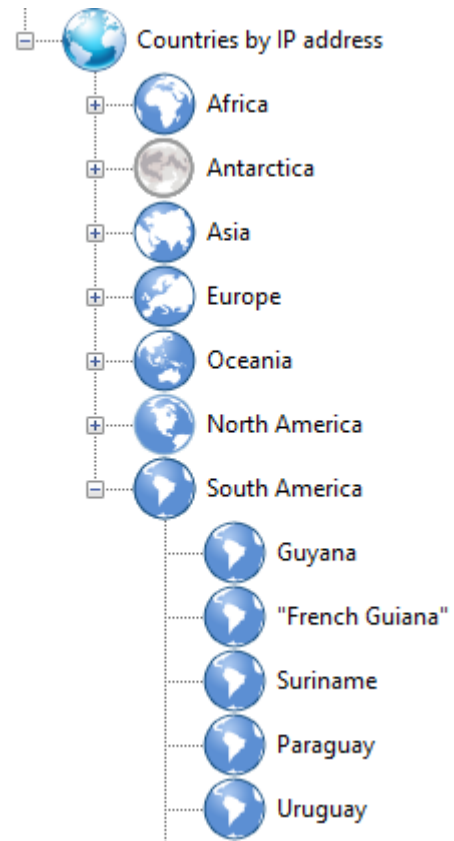
**Change** **Cancel**

## Страны по IP адресу

Internet Administrator detects the country in which the site is physically located by IP address.


For each country assigned specific IP addresses to which you can establish where the site is located physically. This ensures that the contents of the site are under the jurisdiction of the country and should be required to comply with the laws. For example, Russia banned the distribution of pornography, therefore, no one provider in Russia does not allow to post such material and you can guarantee that such materials you will not see.

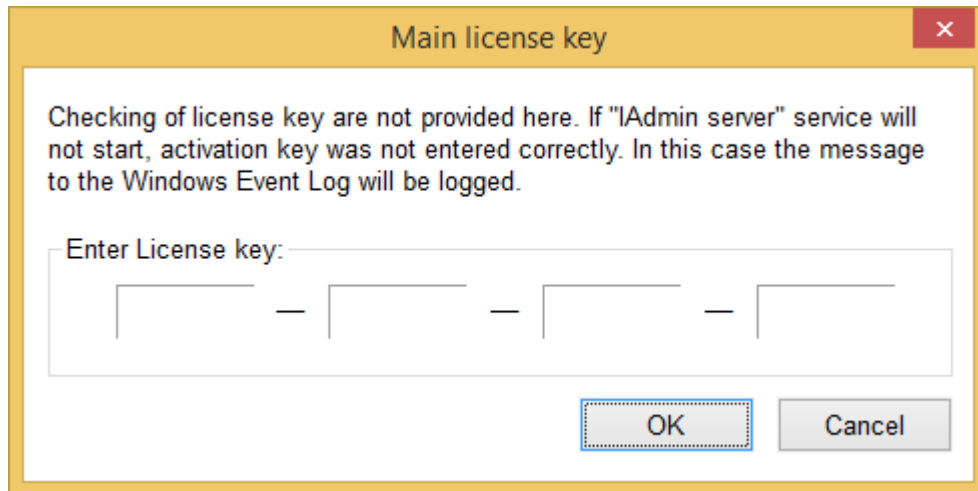
However, it should be kept in mind that popular services can be located outside the required country, and will be restricted, but to such services may be used individually allowing rules!



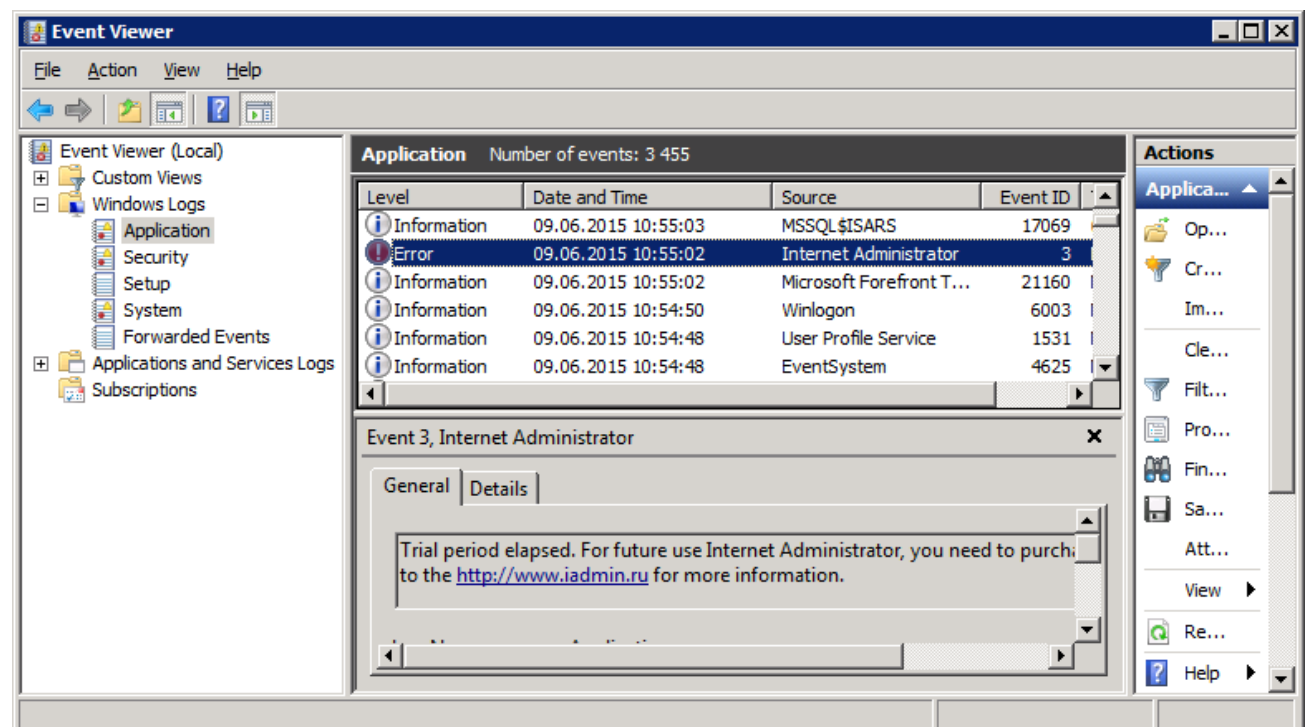
## РАЗДЕЛ 6 – SERVICE

### Section 6.1. – Licensing


You can use the "Internet Administrator" without a license key 60 days after the first installation on the server. After purchasing the software you will get a license key to be entered for further work. The key specifies the maximum number of computers with which the program will work and if this number is exceeded when new computers will automatically added as Unmonitored. You can enter key in the main menu Service -> Main license key or the main toolbar button .

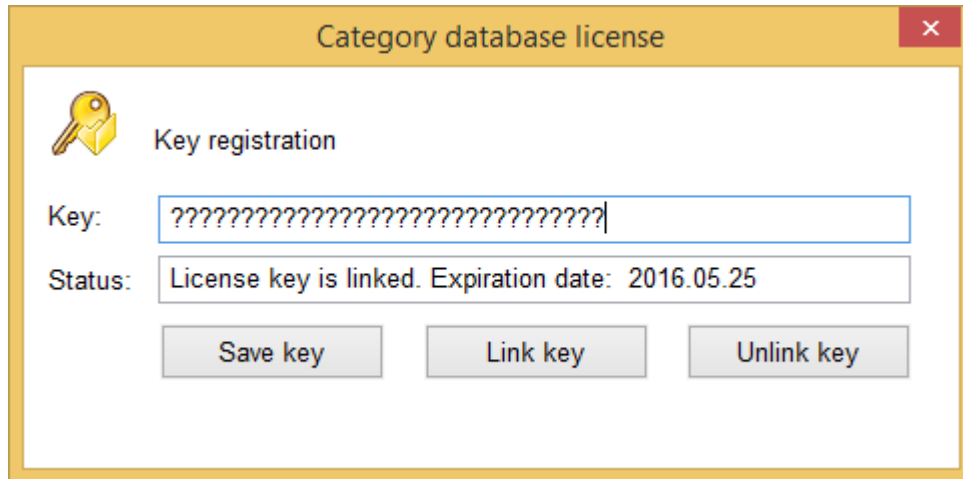


When you enter a key check is not performed, please enter it carefully. Verification occurs during IAdmin Server service startup. If the service does not start, then one of the reasons may be the wrong license key. **In the event of a launch failure Service writes a message in the Applications of Windows event log (available in the Administrative Tools, Event Viewer) under "Internet Administrator" Source.**



## Section 6.2. - Licensing URL Category database

Using categories is available only after you enter the key for Internet Administrator URL Category Database and linking it to the current server. Follow main menu Options -> Category Database Key or main toolbar button  to enter license key.



The dialog box is titled "Category database license" and has a yellow border. Inside, there is a yellow key icon next to the text "Key registration". Below this, there is a "Key:" label followed by a text input field containing 20 question marks. Below that is a "Status:" label followed by a text input field containing the text "License key is linked. Expiration date: 2016.05.25". At the bottom, there are three buttons: "Save key", "Link key", and "Unlink key".

After entering the key, click Save key and then Link key. After successful connection to the Internet Administrator Update server and key verification, it will be linked to the current server.

Linked key cannot be used on another server, for this it is necessary to unlink key from the current server.

Categories operate for a limited time, which determined by the key. At initial purchase key allows you to use a category 1 year from date of purchase. Program will warn for 30 days before the expiry of the key. Upon expiration of the key for future use categories you need to prolong categories for the next period and get a new key. For addition information please see price page <http://www.iadmin.biz/products/?pid=12>.

### Section 6.3. – URL Category database update

Internet Administrator Company will periodically release updates for URL Category database to maintain it up to date. Weekly processed thousands of new porn sites, anonymous proxies and other malicious sites. Updates are available for download only after entering and linking the license key, which also has an expiration date. Updates can add sites, modify a category of existing sites or remove sites from the Category database. The update mechanism is implemented through the management interface and update service IAdmin Update Service. The management interface is opened via the main menu Service -> Category database updates.

Category database management

Automatic updates

☒ Daily ☐ Weekly ☐ Monthly

Sunday

1:00:00

Save changes Update log

Manual update

Status

Current database version: 234

Download now

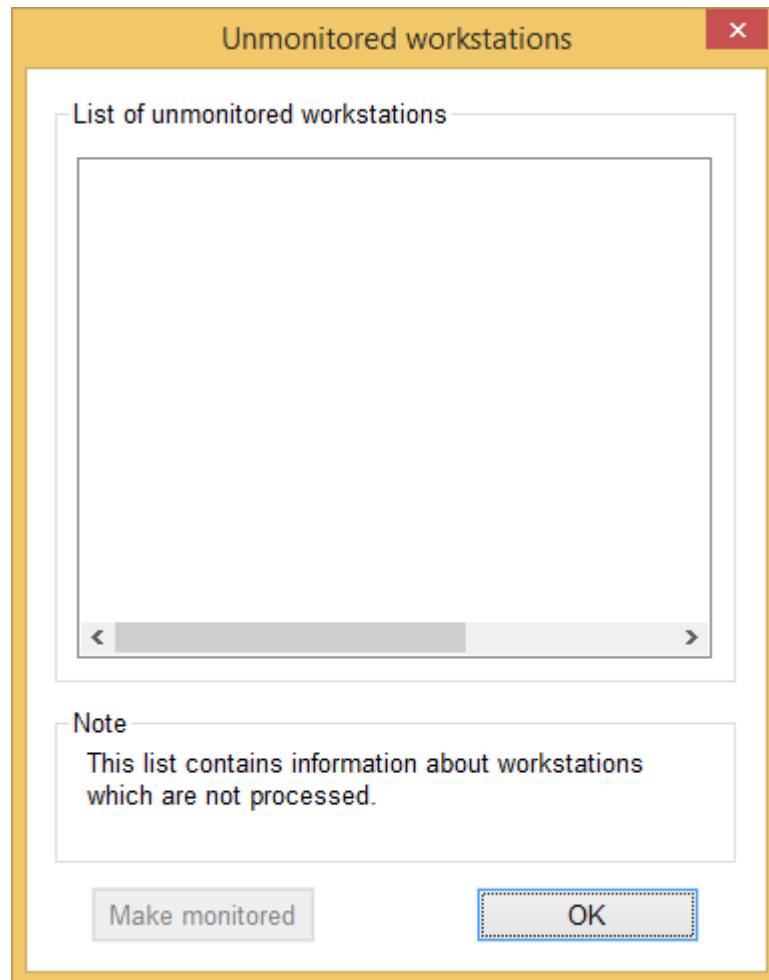
Close

Here you can set period of automatic updates: Daily, Weekly, Monthly, and specify the time of day. This period indicates how often the update service will connect to the update server via the Internet. The results of the automatic updates are logged, which opens on the button "Update log". You can manually start update process by button "Download now". Execution status and results will be displayed in the window.

#### Section 6.4. - Unmonitored workstations

By default, all workstations are monitored and are in the list of workstations main window. Sometimes there is a need to ignore the access policy to certain workstations and network servers. For unmonitored workstations access is not monitored and is not subject to any restrictions.

Addition workstation to the unmonitored list produced from the context menu by highlighting the desired workstation. You can open the list In the main menu Service -> Unmonitored workstations.



From here you can transfer the workstation back to the main list.

If you enter a license key and the number equal to the number of workstations license, the new workstations will be added to the list of unmonitored.

If at the time of entering a license key number of workstations exceeds the number specified in the license, then some of these computers have to transfer to the list of unmonitored. The program will only monitor the licensed count, even if the main list contains more than a license. In this case, it will be difficult to tell which computers are monitored and which are not.



## Section 6.5. - Purge database

**Purge of database**

**Manual purge**

☐ Delete ALL data

☐ Delete all users and computers

☒ Save data for selected period

☐ Today

☐ Current week

☒ Current month

☐ Period from  to

☒ Save numerical traffic and time data

**Purge**

**Auto purge**

☐ Enable auto purge

☒ Every week

☐ Every month

☐ Every quarter

**Save data for selected period**

☐ Last month

☒ Last quarter

☐ Last year

**Save**

**Cancel**

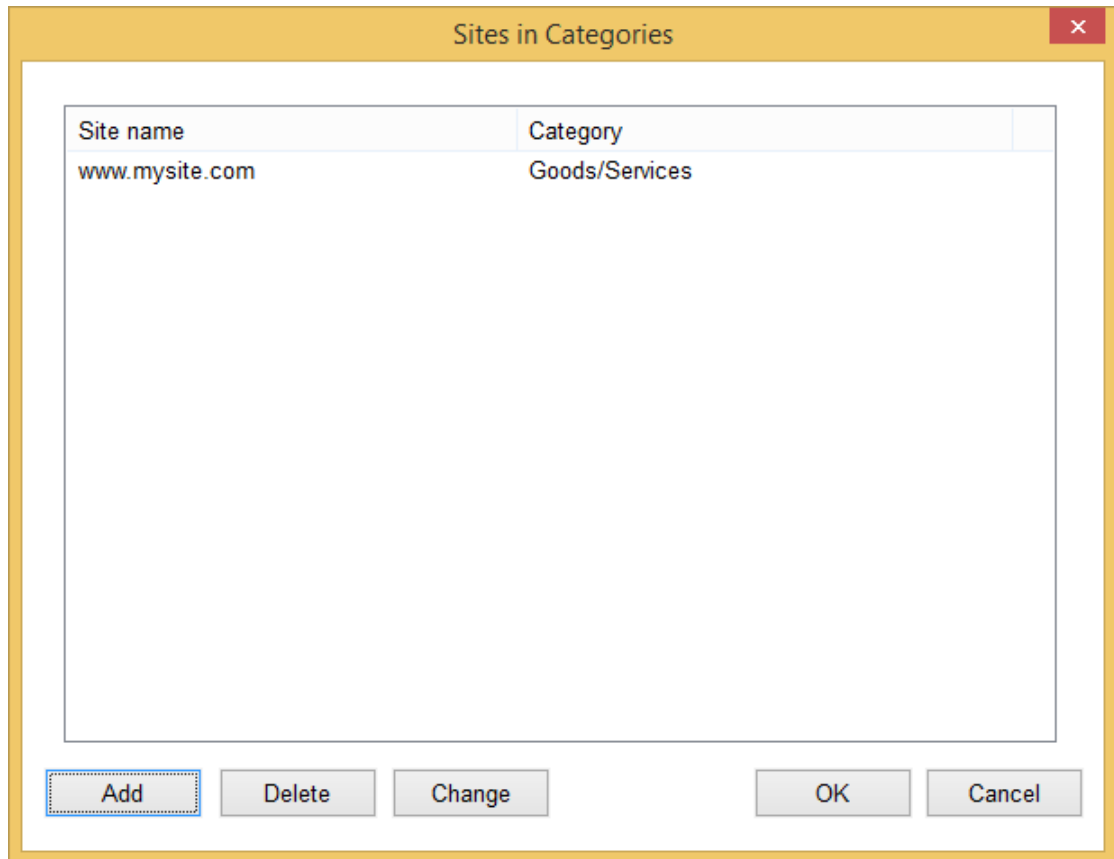
To speed up the database, and to limit the growths the database file on physical media, you can periodically delete outdated information from it. In the menu "Service" select "Purge work database".

You can manually delete all information with users and workstations, or specify a time interval. Save the information is allowed per day over the past week, month, or manually specify the interval.

To configure automatic purging mode, turn it on by checking, and specify the necessary parameters of purge. Automatic purge service carries IAdmin Update Service, cleaning results are written to the update.log file in the program folder.

### Section 6.6. - Custom sites in category

In the menu "Service" select " Custom sites " to open.



The screenshot shows a window titled "Sites in Categories" with a close button (X) in the top right corner. Inside the window is a table with two columns: "Site name" and "Category". The table contains one row with the site name "www.mysite.com" and the category "Goods/Services". Below the table are five buttons: "Add", "Delete", "Change", "OK", and "Cancel". The "Add" button is highlighted with a dashed border.

Site name	Category
www.mysite.com	Goods/Services

This window contains a list of sites and categories are defined using:

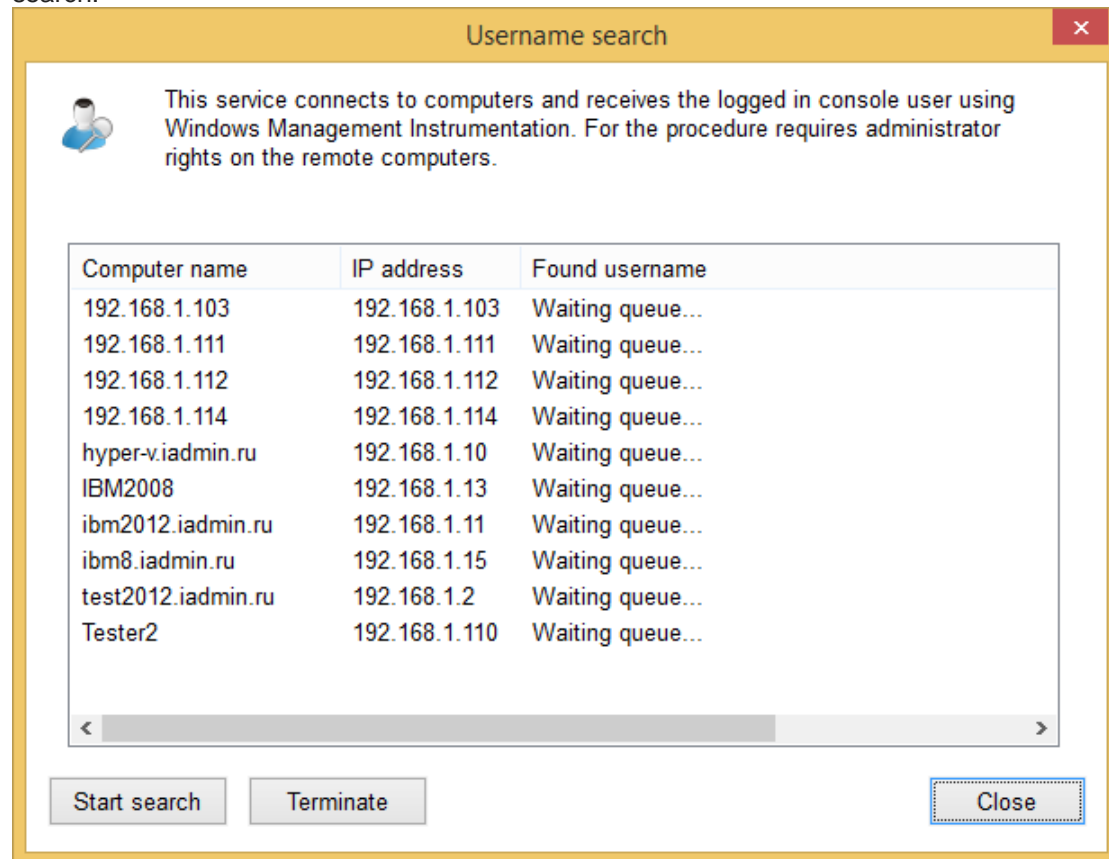
Internet access log and assignment to an existing category.

Adding a site to the custom category, when edit it.

When you delete a site, it will have no category. You can add any site and assign standard or custom categories here.

## Section 6.6. – Username search

Search for user names is available via the Service menu -> Username search.




In the "Static computer" mode, detected computer name is used as username. For a more visual representation use username search for changing of user names in the database. The service will connect to each computer and prompts the logged in user name. This requires administrative rights on each computer, use the domain administrator account.

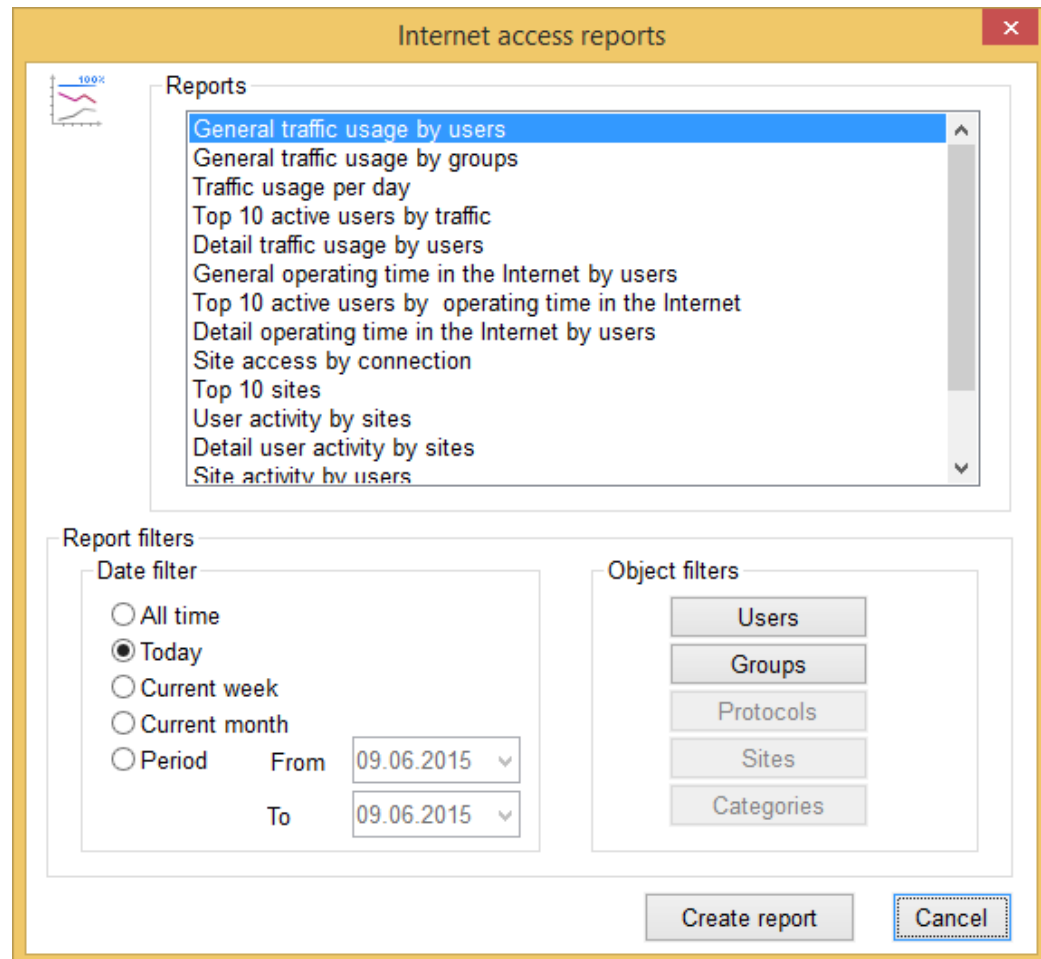
**Do not use this function in the "MS Active Directory" mode!**

## SECTION 7 - Reports

The "Internet Administrator" provides reporting system, showing the dynamics of Internet use in your organization.

### Section 7.1. - Reporting

To open the report window you can use the toolbar button  or select the "Reports" in the main menu "Reports".



To build, click the appropriate report and specify the time period data. Apart from the time the report is possible to specify filters include Users, Groups, Protocols, Web sites and categories.

### Section 7.2. - Customized Reporting

You can customize reports for the following characteristics.

- Users, details of which will be used when generating the report.
- User Groups, details of which will be used when generating the report.
- The time period for which the information will be used to access the Internet. You can specify the following time periods: for all time, today, for the current week or month, and also set the interval manually.
- Access protocols.
- Categories of Web sites.
- The separate sites.

Data filters will be contained in the generated report.

### Section 7.3. - List of reports

The composition and the description of the current reports -  
<http://www.iadmin.biz/products/?pid=10>

### Section 7.4. - Export data to the W3C

In addition to built-in reports Internet Administrator allows you to upload your data to the W3C for the analysis of third-party programs generate reports. To start the export in menu "Reports" choose the "W3C Export".

Specify the file where you want to export the data produced, as well as set the time to upload data collected online by the Administrator. The format of the data in the file is compatible with the format of the log files of Microsoft ISA\TMG Server.

Description of the fields of the export file:

#Fields:	Description
c-ip	User name
cs-username	User name
c-agent	Always set to "Unknown"
date	Date
time	Time
s-computername	Server name, Always set to "IA_Server"
cs-referred	Always set to -
r-host	Site name
r-ip	Site IP address
time-taken	Duration
cs-bytes	Sent bytes
sc-bytes	Received bytes
cs-protocol	Port number
s-operation	Always set to "GET"
cs-uri	URL path
x-action	Access granted or denied
x-category	Site category

## SECTION 8 - DATABASE and Microsoft SQL server

The database of the "Internet Administrator" is the main warehouse.

### Section 8.1. - The default database

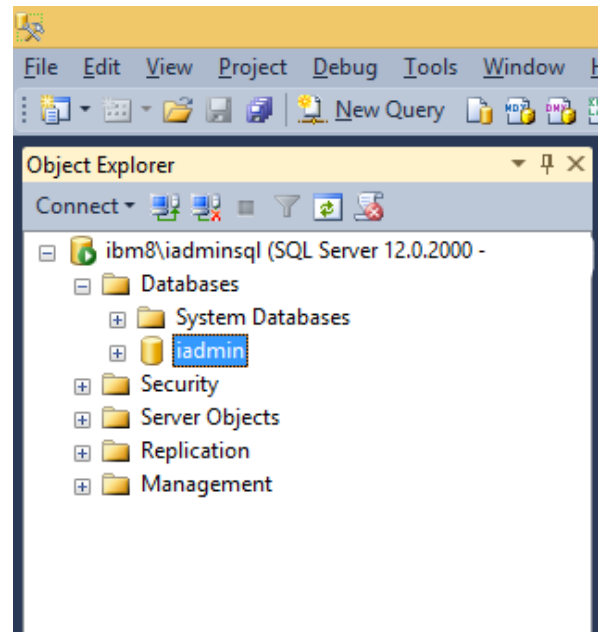
The installation process of "Internet Administrator" installs Microsoft SQL Server Express 2014, creates an ODBC data source and a new database on the installed SQL Server.

To access the database, for example, for backup, it is required additional installation of Microsoft SQL Server Management Studio, available for download from Microsoft.

The database instance is ADMIN SQL on a local server (SQL Server name: localhost \ iadminsql). A Windows user on whose behalf the program is being installed is an administrator of the instance IADMIN SQL.

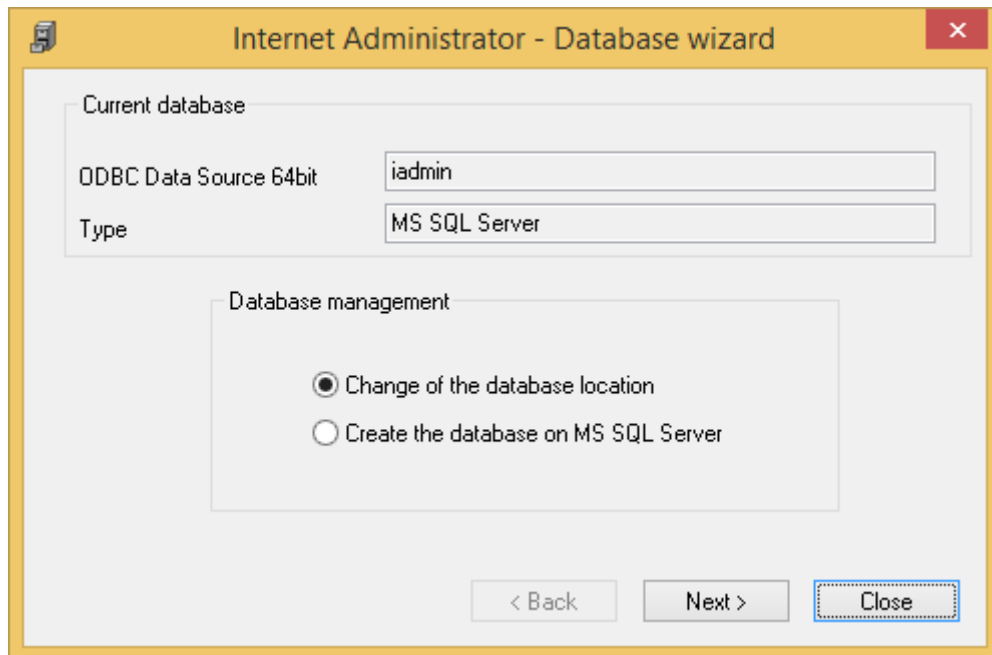
To connect it is used an ODBC data source with the name iadmin, SQL user - sa. If you wish change the sa password in the instance IADMIN SQL, it must be changed via the Database Wizard.

Microsoft SQL Server Express has limitations: supports 1 physical processor, 1 GB RAM and 10 GB of disk space. SQL Server Agent and functions associated with it is not available. To remove the Express limitations use a Microsoft SQL Server.



## Section 8.2. - MS SQL Server Database

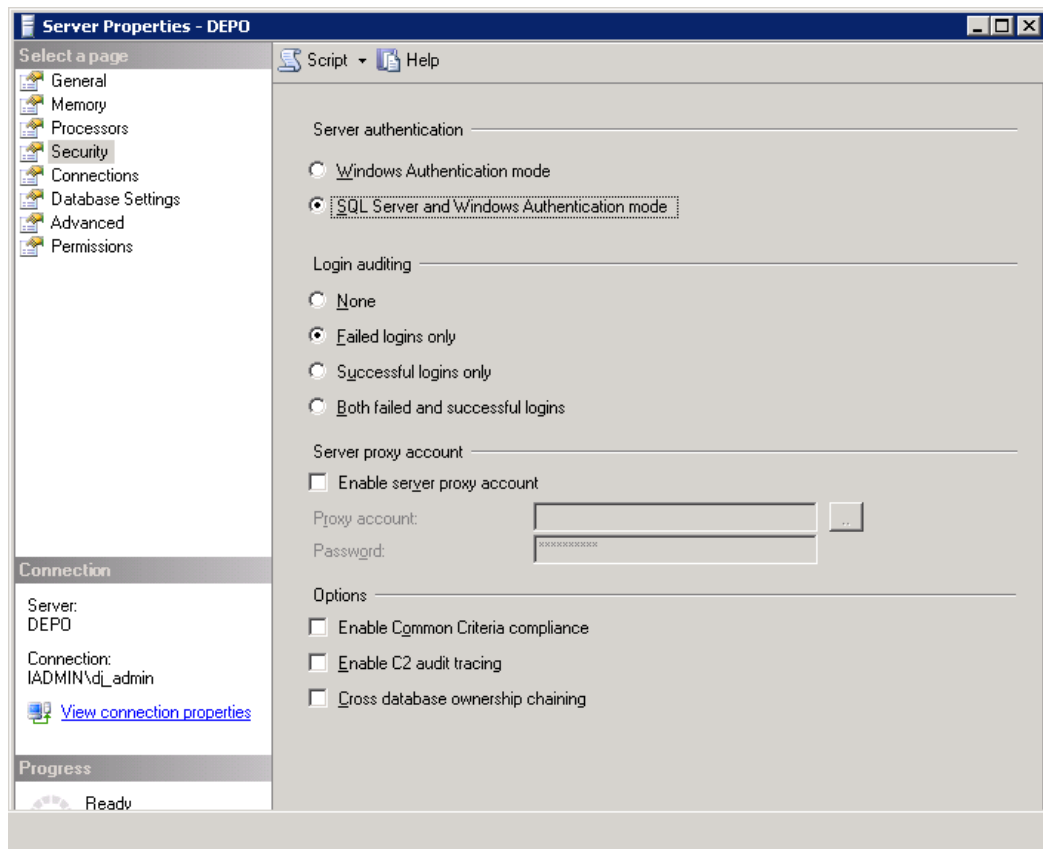
Internet Administrator can use Microsoft SQL Server as the database management system. Internet Administrator includes “Database wizard” to manage database connection.



The wizard can create a database on MS SQL Server and change the database to use.

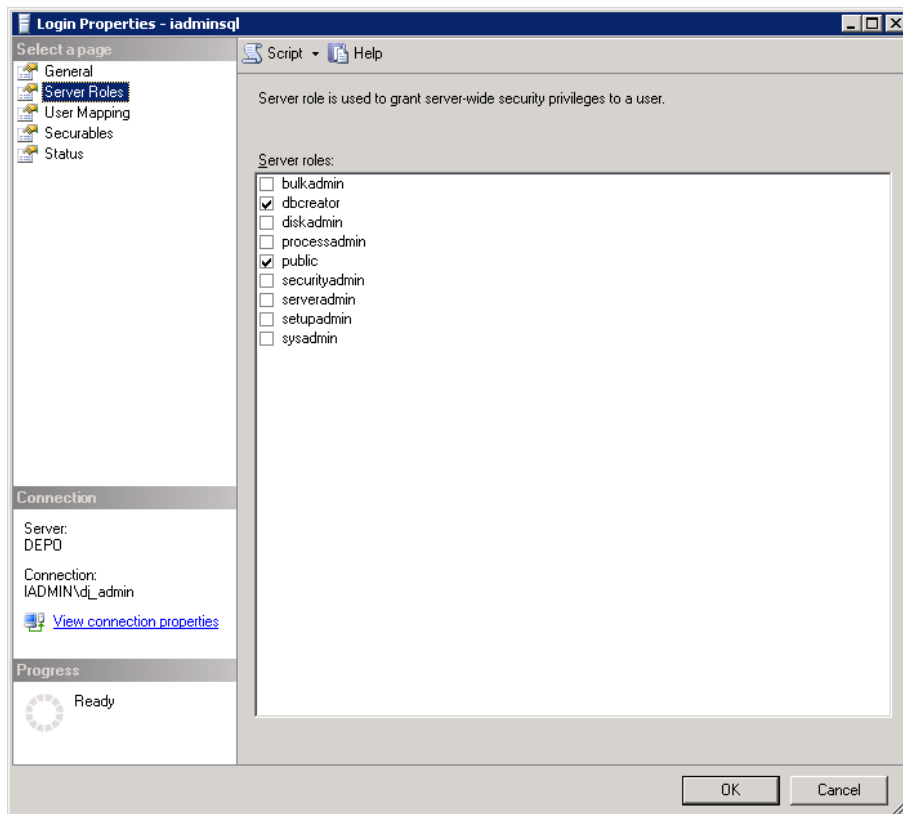
## Creating a database for MS SQL Server

In MS SQL Server properties set mixed authentication mode (SQL Server and Windows).

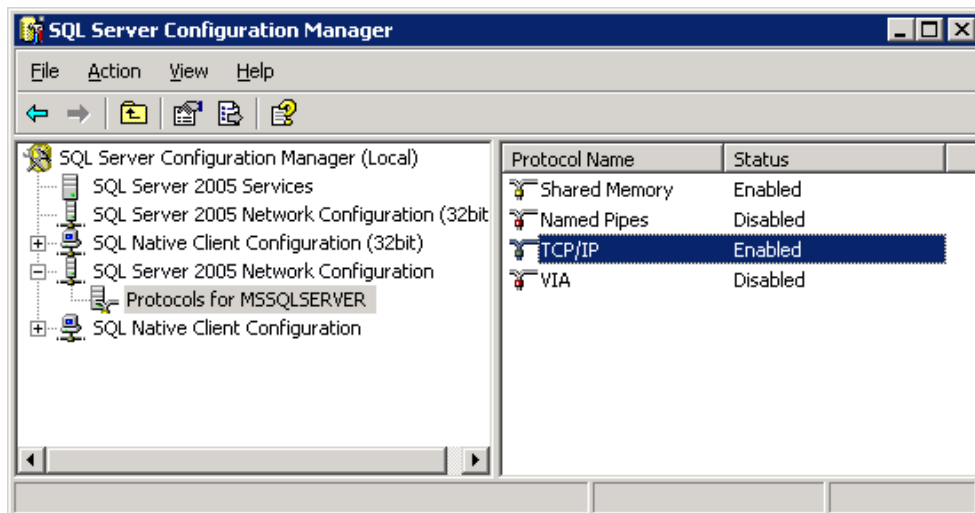




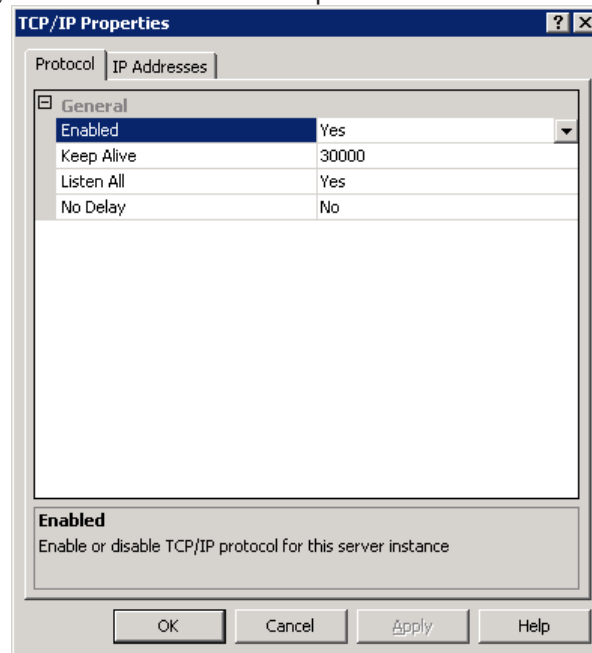
Create a user and on the Server Roles tab enable “dbcreator” user role, that it could create a database.



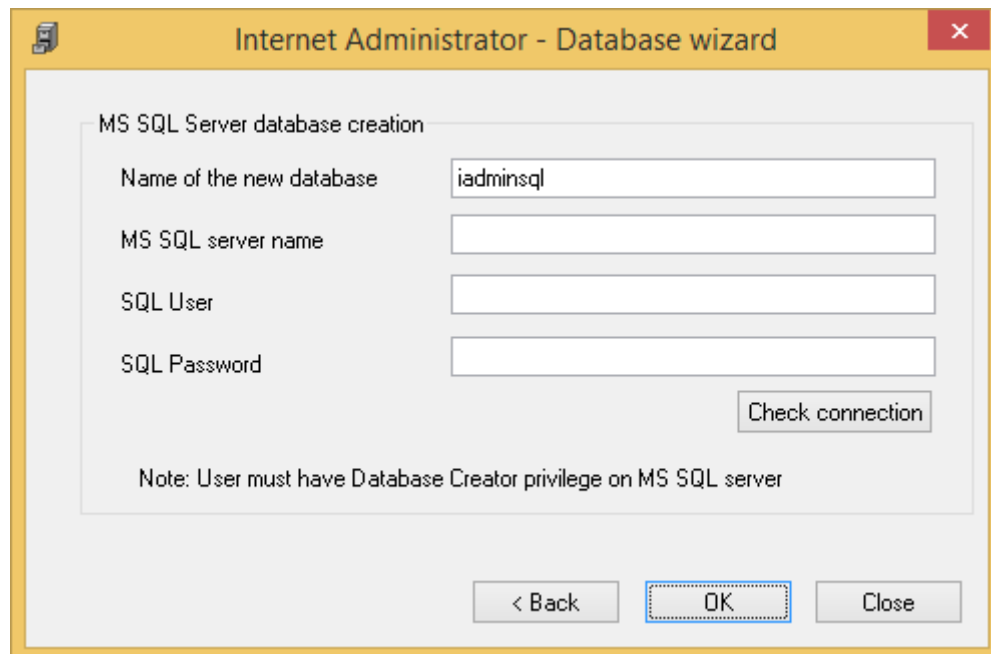
If SQL Server installed on a remote server, you need to enable network support. Run the utility “SQL Server Configuration Manager” in SQL Server program group, subgroup Configuration Tools, and then expand SQL Server Network Configuration.



Open the properties of TCP / IP and enable its support for remote connections, if they are disabled. Also, enable TCP / IP to the required IP address in the next tab.



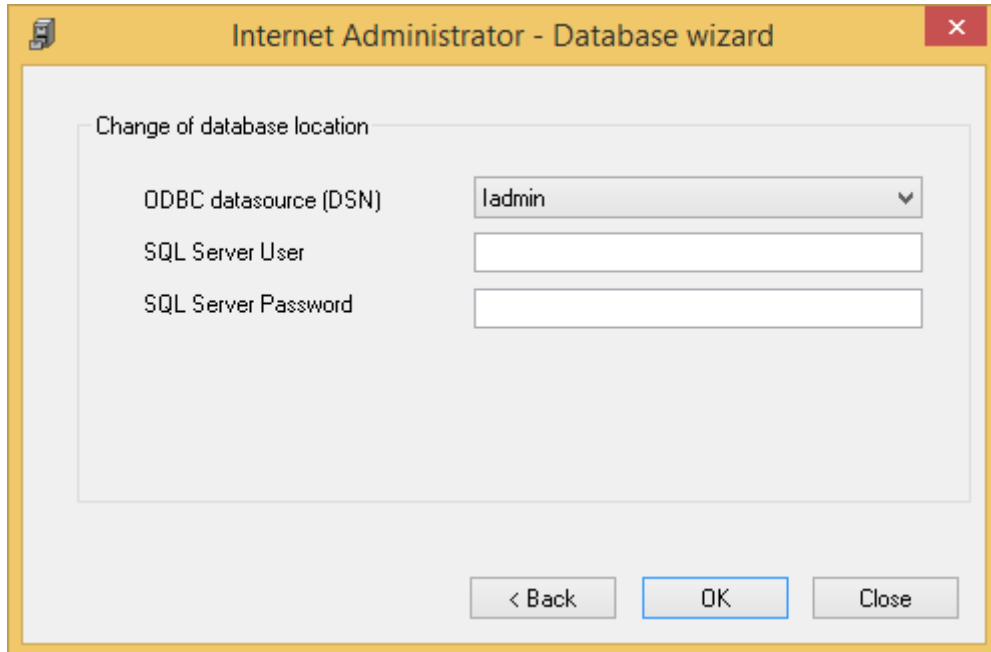
Now run the "Database Wizard" and select "Create the database on MS SQL Server». On the next screen, enter the name of the new database, the name of the SQL server instance and SQL name and SQL password of the user created above. The database name must be unique to the selected instance.



By clicking on the "Finish" button the wizard will make an attempt to create the database and report the results. **For the changes to take effect, restart IAdmin Server service and Rules Administrator program.**

## Change a database

To change the connection settings of the database select "Change the location of the database" in the "Database Wizard".



Internet Administrator - Database wizard

Change of database location

ODBC datasource (DSN) Iadmin

SQL Server User

SQL Server Password

< Back OK Close

The data source for MS SQL Server is created when you create a new database. If the ODBC source is created manually, its name must necessarily match the name of the database. **For the changes to take effect, restart IAdmin Server service and Rules Administrator program.**

### Section 8.3. – Backup

To prevent data lose collected by "Internet Administrator" we recommend to back up the database. Backup is performed by MS SQL Server. To set up and more information, refer to the documentation for MS SQL Server.

## SECTION 9 - Distributed network and Collectors

"Internet Administrator for Network" includes tools for the construction of a single scheme of monitoring and policy management of Internet access for distributed networks. This is achieved by creating a central database, and the installation of Internet Administrator copies to each of the monitored network or for each server acting as a gateway. By distributed network is meant networks that are in different physical networks, separated by routers in different buildings or having different Internet connections.

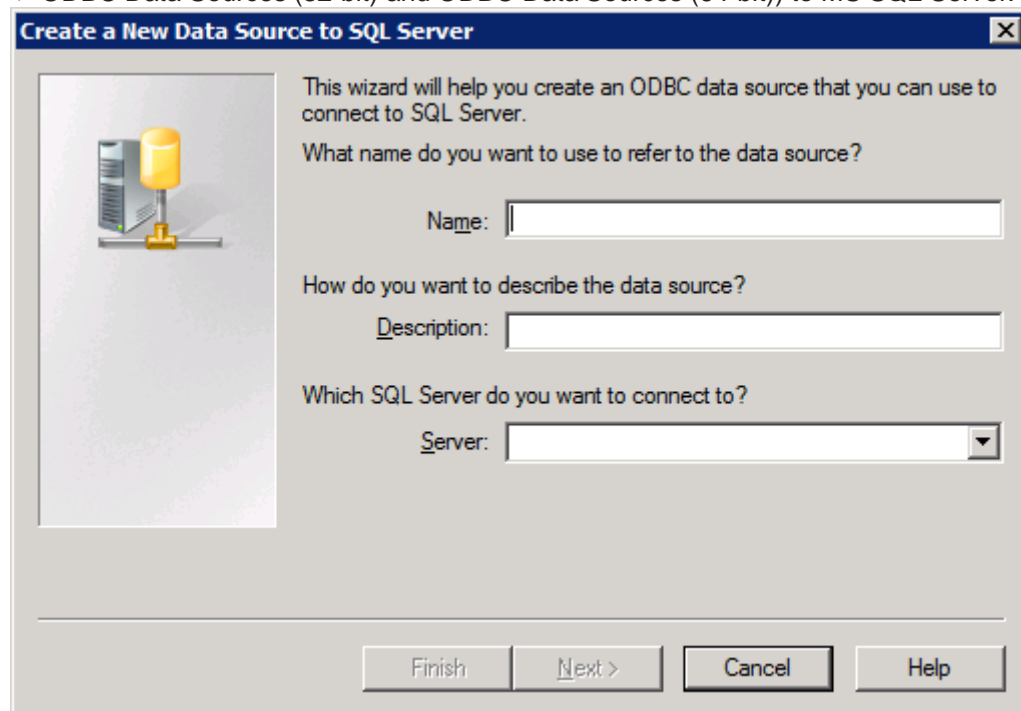
### Section 9.1. - Central data warehouse

To create a central data warehouse is necessary to make the first installation in the central network and migrate the database to a Microsoft SQL Server (see. Section 8). In this database it will store all the information, settings and access rules for all other collectors.

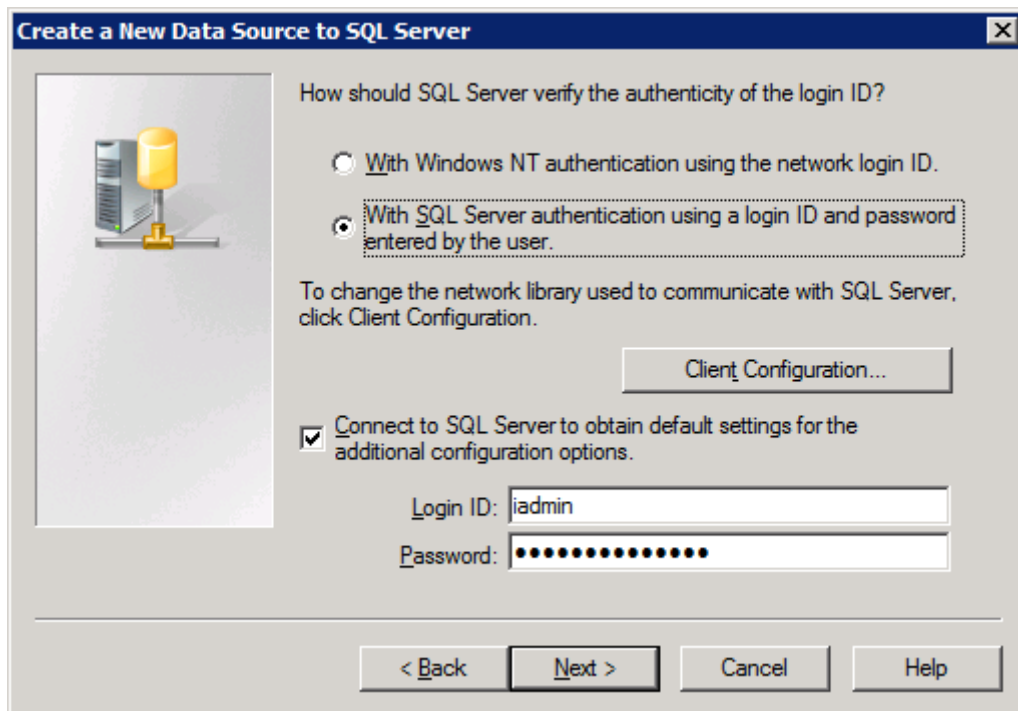
### Section 9.2. - Installation of additional collectors

Install "Internet Administrator" on the remote network in the usual way, stop the "IAdmin Server" service. To connect to the central database, "Internet Administrator" need access to MS SQL Server in a central network.

Create two identical ODBC data source for 32 and 64 bit applications (Administrative Tools -> ODBC Data Sources (32-bit) and ODBC Data Sources (64-bit)) to MS SQL Server.



As a data source name, specify the name of the database on a central server. If the database is called "ladmin", then you need not create just modify existing data sources ladmin for 32 and 64 bit connections. As a server, specify the name of the MS SQL Server instance in a central network. Set SQL Server user authentication.



Test the data source before you create.

Then, using the utility "Database wizard", change the location of the database and select new created data source. Specify a name and password that were entered when creating a database in the central network.

Start (or restart) the IAdmin Server service. If the service is started up without error, the connection to the central database is successful.

**NOTE! In remote networks must be different IP addressing. That is, there should not be two computers with the same IP address, IP network should not be crossed. At the intersection of IP networks to a single user will be recorded traffic from all computers on other networks with the same IP address, which is set on his workstation.**

### Section 9.3. - Administration

After the creation of a single scheme, you can use any collector of any network to access control, view statistics and create reports. But for the normal operation from the place of administration is necessary, that there was a connection to all the servers through the DCOM protocol over RPC. It is advisable not to filter traffic via VPN, because it always uses the RPC dynamic ports. Also, you must configure the name resolution of servers that is hosting the "Internet Administrator".

In carrying out some actions in an administrative utility, such as blocking the user commit changes to the rules, etc. communication occurs every collector with Internet Administrator. If such a connection can not be established, the changes will be applied only in the database, and the remote Collector will apply them only after you restart the IAdmin Server service on it.