

Aker Web Content Analyzer

Configuration Manual

- Introduction

- 1-0 Installing Aker Aker Web Content Analyzer
 - 1-1 Hardware and software requirements
 - 1-2 Installing the URL Analyzer

- 2-0 Configuring Aker URLs Analyzer
 - 2-1 Basic configurations
 - 2-2 Additional configurations
 - 2-3 Other options

- 3-0 Using the Firewall - 1 Plugin
 - 3-1 Introduction
 - 3-2 Configuration
 - 3-3 Logs

- 4-0 Using the Squid plugin
 - 4-1 Introduction
 - 4-2 Squid Configurations
 - 4-3 Plugin configurations
 - 4-4 Access Profiles and Rules
 - 4-5 Profile selection

- 5-0 Using the ISA Server plugin
 - 5-1 Introduction
 - 5-2 Installing the plugin
 - 5-3 ISA Server Configurations
 - 5-4 Plugin configurations
 - 5-5 Access Profiles and Rules
 - 5-6 Profile selection

- Appendix A - Log Messages

- Appendix B - Copyrights and Disclaimers

Introduction

This is the Aker Web Content Analyzer user's manual. In the next chapters you will learn how to configure this powerful tool for access control. This introduction intends to describe this manual organization and try to make its reading as simple and comfortable as possible.

What is Aker URL Analyzer?


Aker URL Analyzer is a powerful tool to control access to Internet sites, when operating along with a firewall or proxy server.

The product consists in a huge database with Internet URLs classified in one or more categories with automatic and daily update from Aker Security Solutions. This way, it is possible for an administrator to configure what sites categories specific users will be allowed to access, without the concern of manually registering them. It allows the staff productivity to increase, as they will stop accessing information that is useless for their work, at the same time it decreases the traffic over the Internet link, reducing the necessity of upgrades and thus saving money.

How this manual is disposed.

This manual is organized in several chapters. Each chapter will present one aspect of the product's configuration and all relevant information about the aspect in focus.

It is recommended to entirely read this manual at least once, in the presented order. Subsequently, if necessary, it can be used as a reference source (to facilitate its use as reference, the chapters are divided into topics, with direct access by the main index. This way, it is possible to easily find the desired information).

In several places of the manual, the symbol  followed by a red colored sentence will appear. It means that the refereed sentence is a very important observation that must be entirely understood before continuing to read the chapter.

System's Copyrights

- Copyright (c) 2001 Aker Security Solutions
- This product uses the MD4 algorithm from RFC 1320. Copyright (c) 1991-2 RSA Data Security, Inc.
- This product uses the MD5 algorithm from RFC 1321. Copyright (c) 1991-2 RSA Data Security, Inc.

1-0 Installing Aker URL Analyser

This document presents how to install and remove Aker URL Analyser.

1-1 Hardware and Software requirements

Aker URL Analyser runs on Windows (NT 4.0, 2000 Server e 2003 Server), Linux (Red Hat 7.3, 8, 9 and Conectiva 8, 9) operating systems, on Intel 32 or compatible platforms. It is compatible with Aker Firewall from version 4.0 on, MS Proxy Server, MS ISA Server, Checkpoint Firewall 1 and Squid Internet Object Cache. Except for the Aker Firewall, plugins are necessary to connect to the other software.

For a satisfactory performance, Aker URL Analyser requires the following hardware:

- Processor Pentium 233Mhz or higher

If there is a large number of clients accessing the URL analyser, a machine with faster processing capacity can be required.

- 64 Mbytes of RAM

The use of 128Mbytes is recommended for all installations.

- 50 Mbytes of disk space
- Monitor
- Network adapter(s)

It is important to emphasize that all the hardware devices must be supported by the installation O.S.

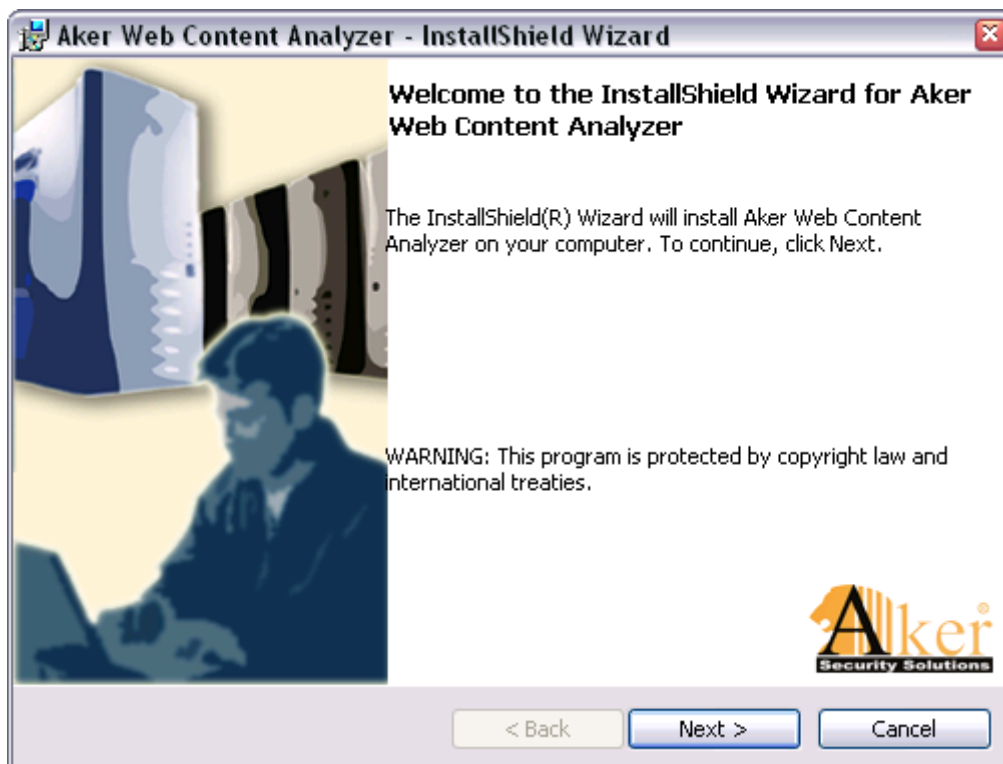
1-2 Installing the URL Analyser

1-2-1 Instalng in Windows Servers

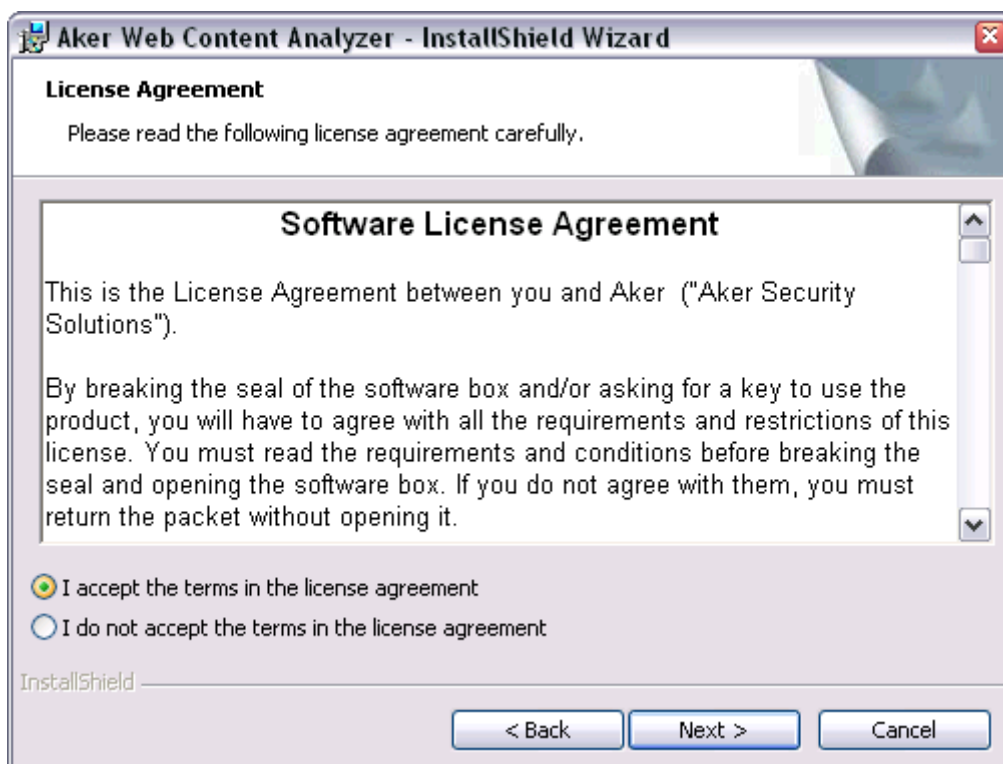
The installation procedure is quite straightforward. Just follow the steps bellow:

1. Click the **Start** menu button
2. Select the **Run** option
3. When asked about which program to run, type
`webcontentanalyzer_win_en_version.exe`

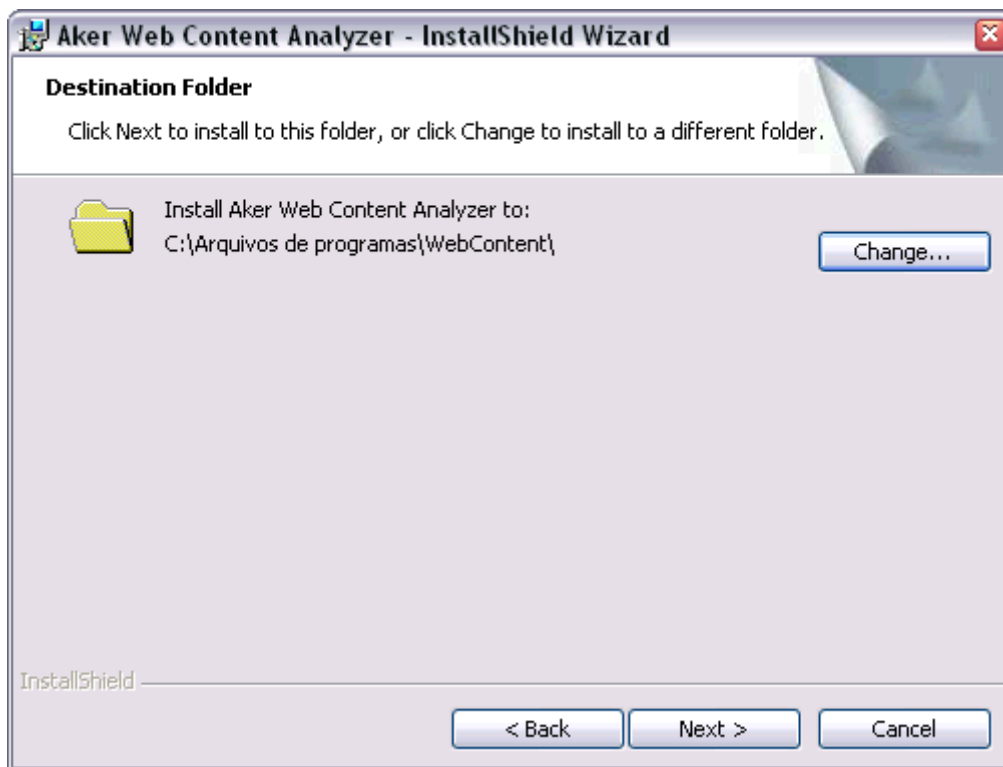
The window bellow will be displayed, being necessary to click on the *Next* button to proceed with the installation:



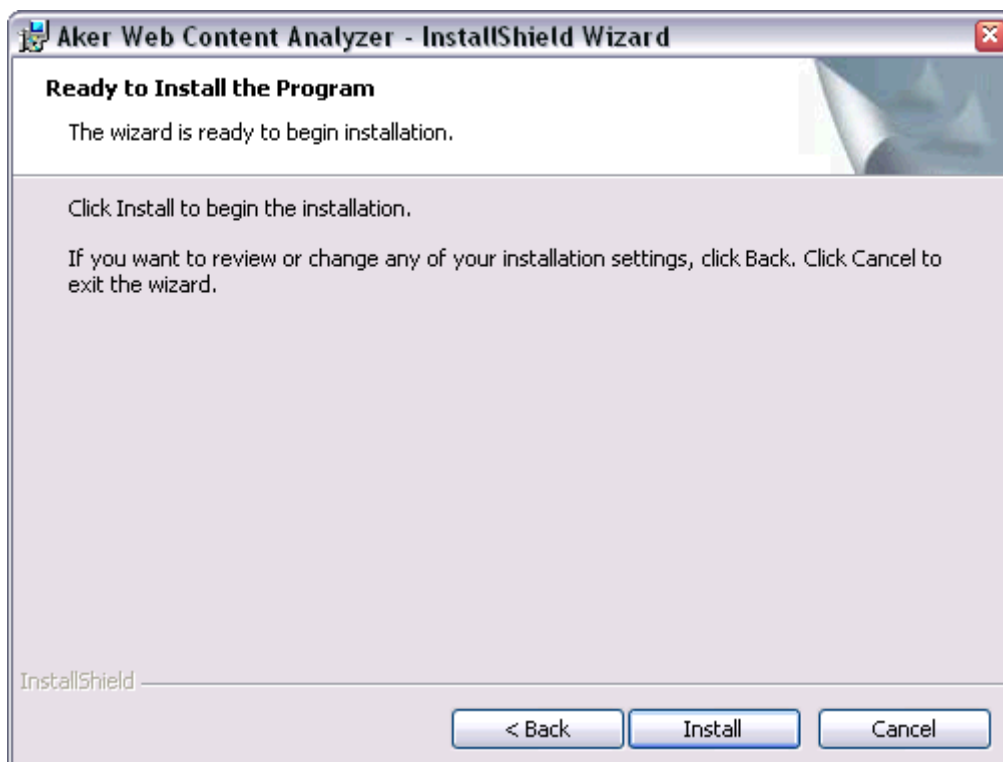
The next screen shows the licensing agreement. In order to have the installation proceed, select the option **I accept the terms in the license agreement**, after carefully reading it. If you don't accept, the installation will abort.



Choose the installation folder.



Press *Install* to have the program installed, according to your previous choices.



1-2-2 Removing from Windows Servers

To remove the Aker Web Content Analyzer from your computer, please choose the option *Add or Remove Programs* in the Windows Control Panel. Look in the list for the Aker Web Content Analyzer entry and click *Remove*.

1-2-3 Installing in Linux Servers

The Aker Web Content Analyzer for Linux comes as a standard RPM package. To install it, the user may use a graphical package manager or use the standard, text-based RPM tool:

```
rpm -ivh package_name.rpm
```

Adicional packages may have to be installed as a dependency, such as the QT libraries. They can be downloaded from the Aker website (www.aker.com.br) or installed directly from the product installation CD.

1-2-4 Removing from Linux Servers

The Aker Web Content Analyzer for Linux comes as a standard RPM package. To remove it, the user may use a graphical package manager or use the standard, text-based RPM tool:

```
rpm -e package_name
```

1-2-5 Installing in FreeBSD Servers

The Aker Web Content Analyzer for FreeBSD comes as a standard FreeBSD package. To install it, the user may use a graphical package manager or use the standard, text-based *pkg_add* tool:

```
pkg_add package_name.tgz
```

Adicional packages may have to be installed as a dependency, such as the QT libraries. They can be downloaded from the Aker website (www.aker.com.br) or installed directly from the product installation CD.

1-2-6 Removing from FreeBSD Servers

The Aker Web Content Analyzer for FreeBSD comes as a standard FreeBSD package. To remove it, the user may use a graphical package manager or use the standard, text-based *pkg_delete* tool:

```
pkg_delete package_name
```

2-0 Configuring Aker URL Analyser

This document presents how to configure Aker URLs Analyser.

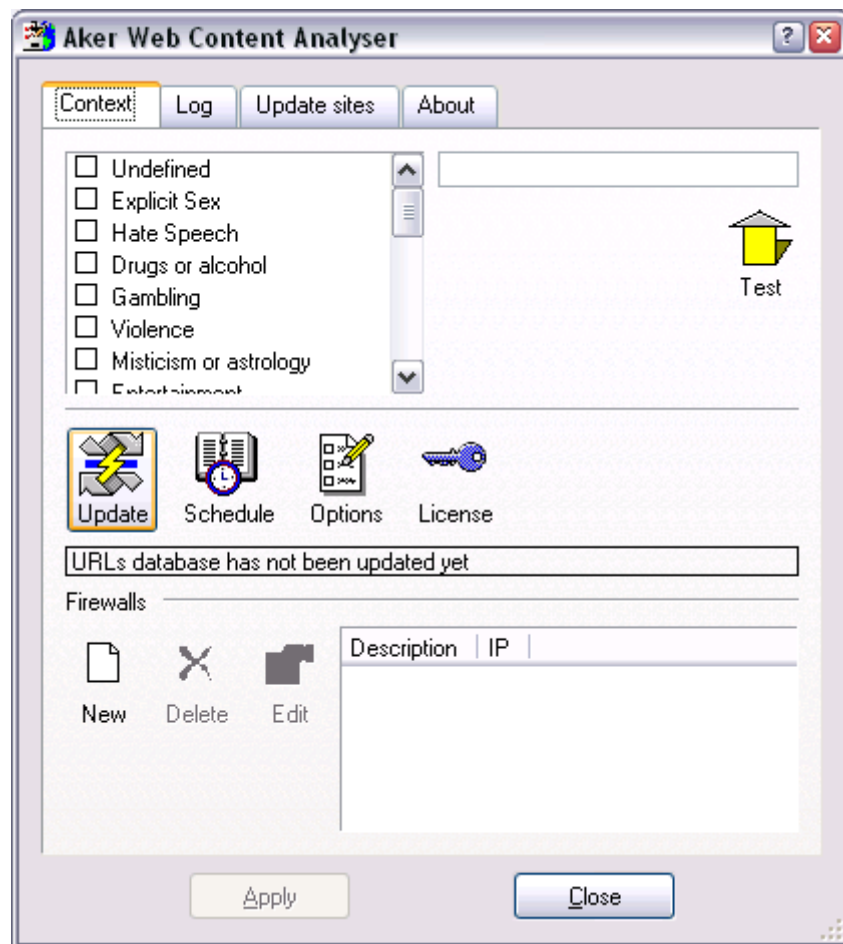
2-1 Basic configurations

Aker URL Analyser runs as a operating system service. To configure, it is necessary to start the its graphic user interface.

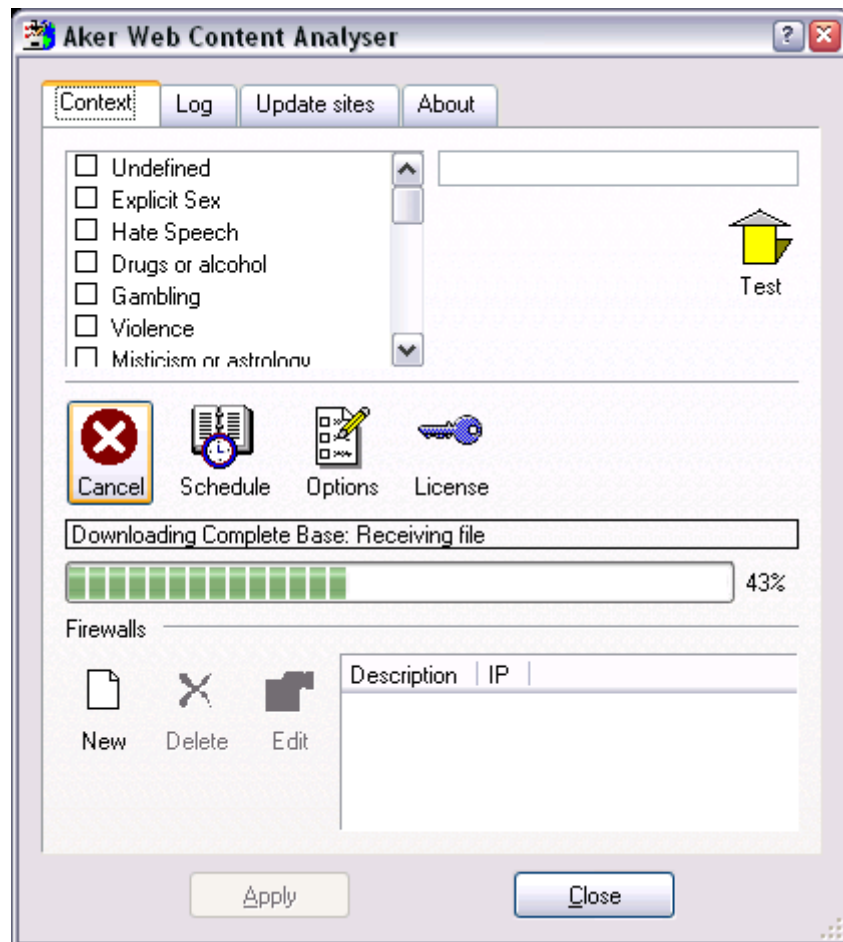
In order to start the graphic user interface just perform the following steps:


- In **Windows**:
 - Click on the **Start** menu button, select **Aker Firewall** group, inside it select the sub-group **Web Content Analyser** and finally click on the program name.
- In **Linux** or **FreeBSD**, inside an X environment console, type:
`/usr/local/akerurl/akerurl_conf &`

The following window will appear:



The first action to be performed by the Administrator is the URLs base update. This is necessary since the database that comes along with the product will certainly not be updated and many new URLs will not be listed. To proceed with the update, click on the **Update** button, located in the toolbar. After a confirmation dialog, please observe that the **Update** option has changed to **Cancel**, allowing the user to stop the updating process at any moment. The updating process is displayed in a progress bar, as showed in the picture below:



 The first base update can take a while, depending on the Internet connection speed. The following updates will be much faster, as only the base differences will be transferred.

The next step to configure the analyser will be the registration of the firewalls that will access it. In order to do it, click on the **Include** icon, in the toolbar of the **Firewalls** group.

The following window will be displayed:



IP: Is the IP address of the firewall that will access the URL analyser.

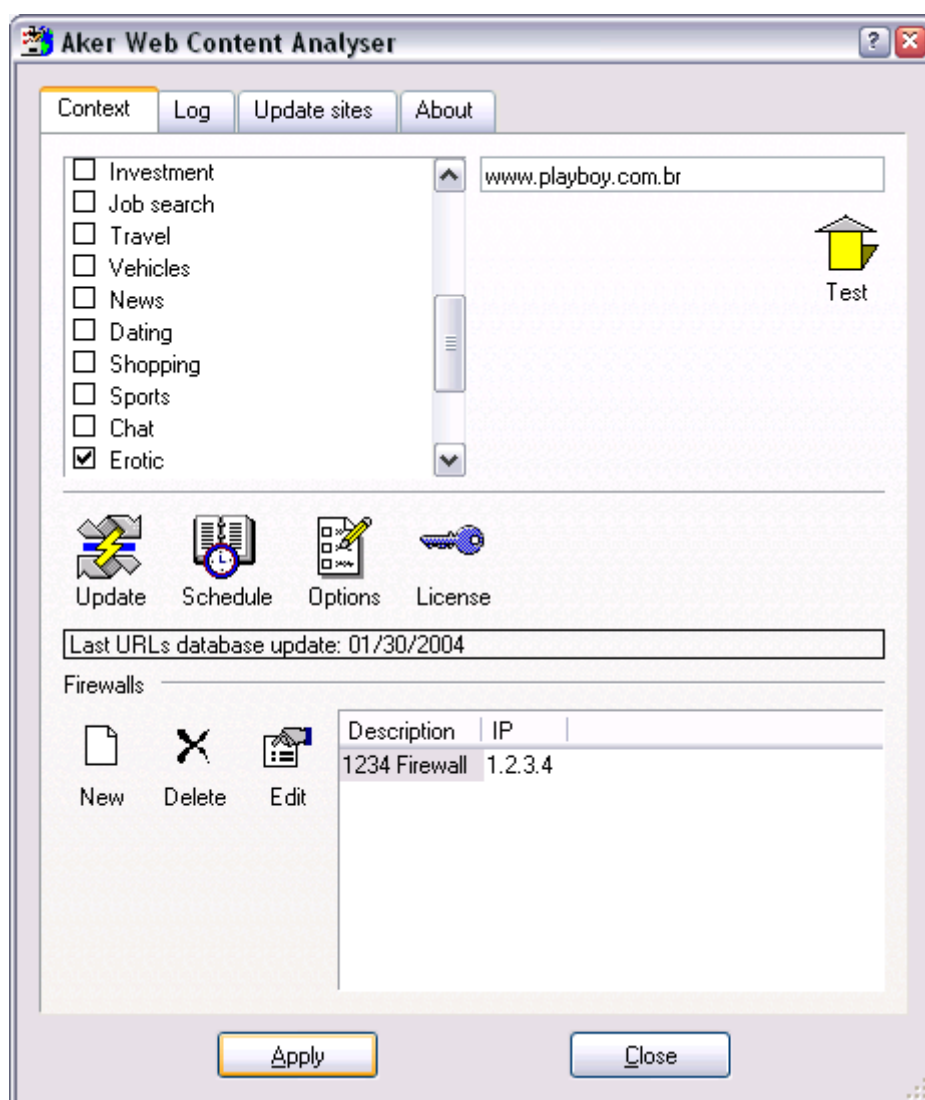
Description Is a free text field, used only for documentation purposes.

Password: Is the password used to create the authentication and encryption keys, used in the communication with the firewall. This password must be the same as the one configured in the firewall.

Confirmation:: This field is only used to verify if the password has been typed correctly. It is required to type it exactly as the one in the *Password* field.

Observe that it is possible to **Edit** or **Exclude** the registered firewalls at anytime, by clicking in the correspondent button in the toolbar.

 After the desired changes have been done, it is necessary to click on the **Apply** button.

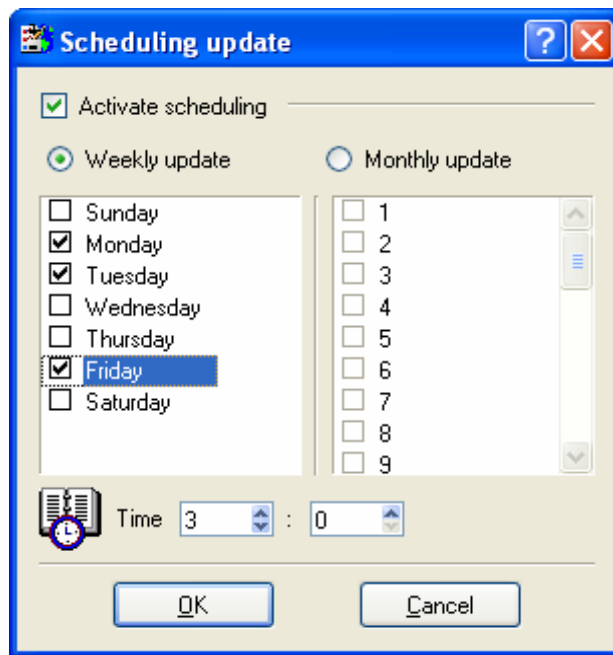


2-2 Additional configurations

In this section will be presented the advanced configuration options of Aker URL Analyser. They are:

- **Schedule**

By clicking on the **Schedule** option, located in the toolbar, it is possible to define the days and the time when the automatic updates will take place. By clicking on this option, the following window will be displayed:

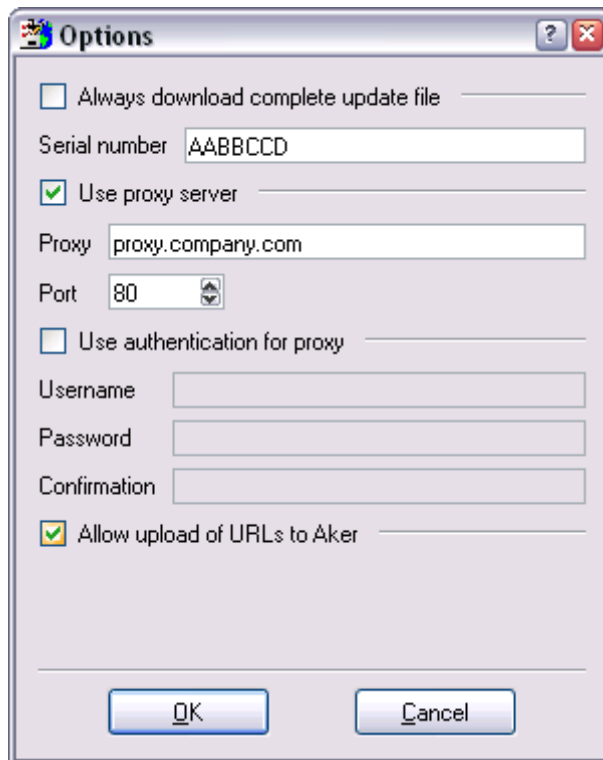


The **Activate scheduling** option, if checked, will make the URL Analyser to automatically download the database updates. If it is not checked, the updates will only be performed manually.


The **Weekly update** and **Monthly update** options allow the definition of the week days or month days when updates will happen.

- **Options**


This option allows the definition of additional parameters of Aker URL Analyser functioning. By clicking on it, the following window will be presented:



The **Always download complete update file** option, if checked, will make the URL Analyser to always download the entire base, instead of only the differences.

 This option must only be used in case of problems, as downloading the entire base will cause a useless increasing in traffic and download time.

The **Serial number** field allows the verification and modification of the product's serial number.

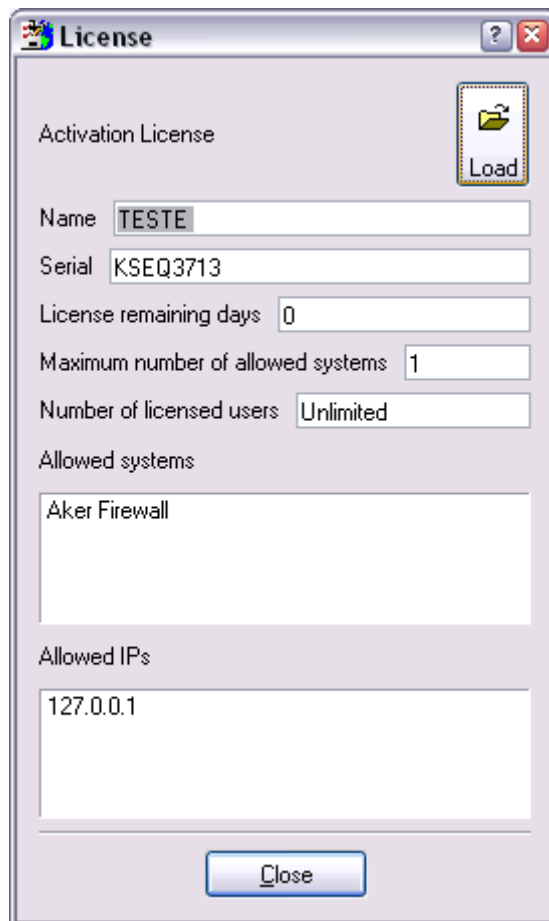
 The serial number must only be changed if solicited by Aker Security Solutions technical support, under the penalty of stopping the product operation.

Web Proxy: If it is necessary to use a web proxy to download the database and its updates, it is possible to specify the access name and password that Aker URL Analyser will supply to the proxy.

 The URL analyser uses the same proxy configurations as defined in the operating system control panel.

- **License**

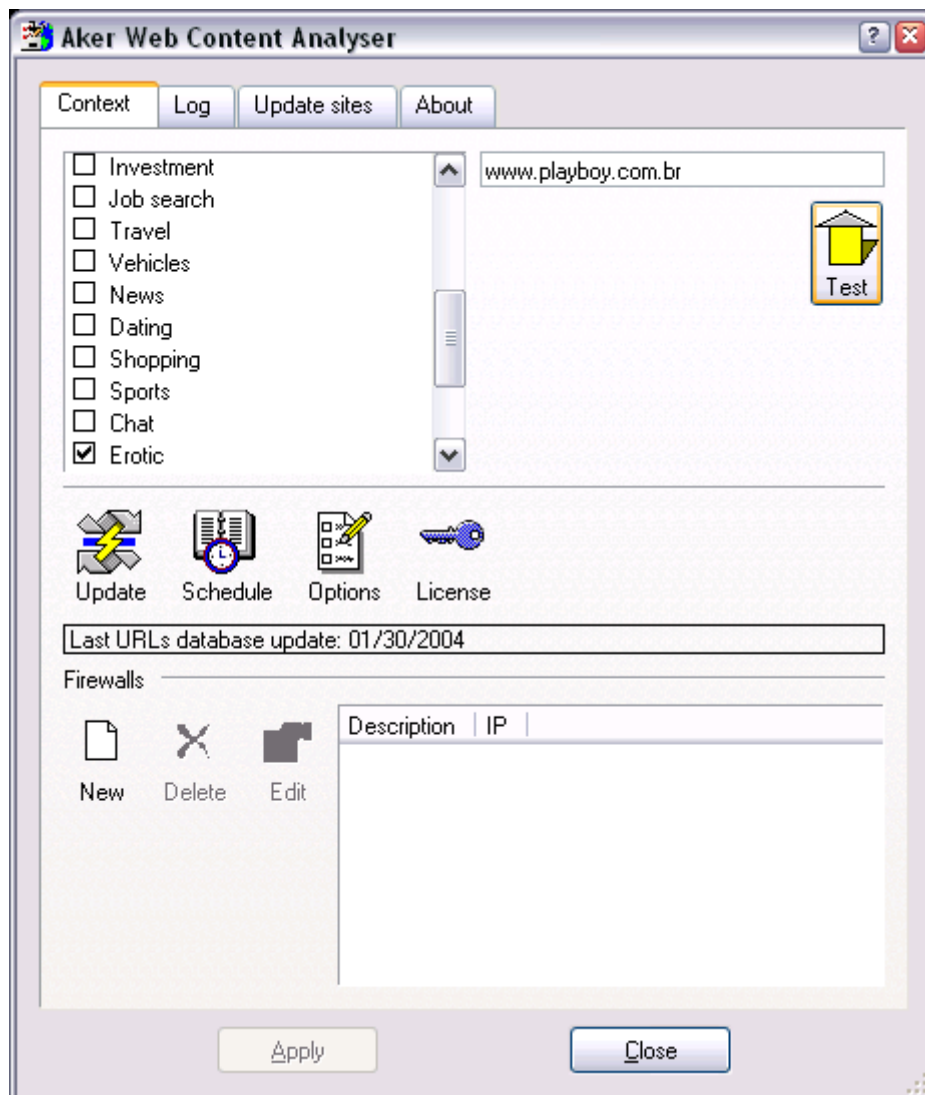
This option allows the visualization of the present license data, and the loading of a new one. By clicking on it, the following window will be displayed:



To load a new license, just click on the **Load** button, located on the top of the window. After it, a new window will be shown, where it is possible to specify the name of the file with the license.

- **URLs test**

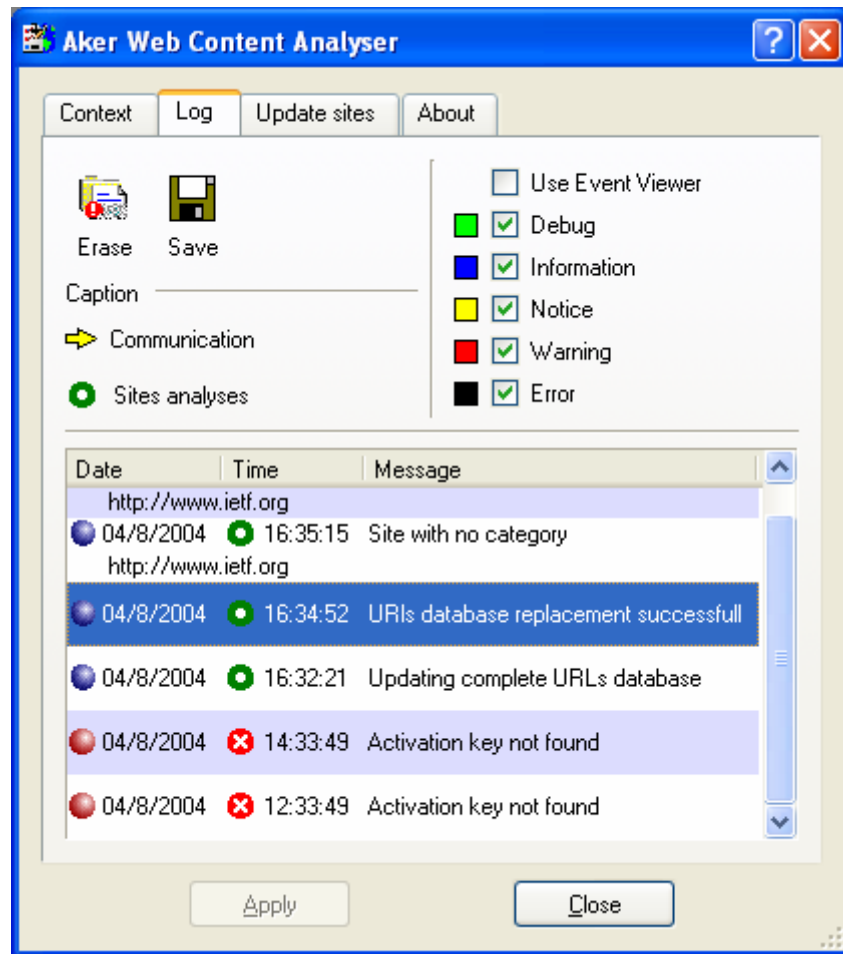
The administrator will be able to check the classification of a URL at anytime just by entering the desired address in the test field, located in the right top of the window, and clicking on the **Test** button. If the site is classified, the classification will be presented in the field at the right of the window. If it does not have a classification, all the category fields will be presented in blank.



2-3 Other options

In addition to the main tab, where all the functioning aspects of Aker URL Analyser are configured, there are three other tabs where it is possible to obtain additional information about the product and its functioning. They are:

Log



This folder is useful to verify Aker URL Analyser functioning. It consists of a list with several messages, each one presented in alternated colored lines, in a way to facilitate their identification. On the right of each message there is a colored square that represents its importance.

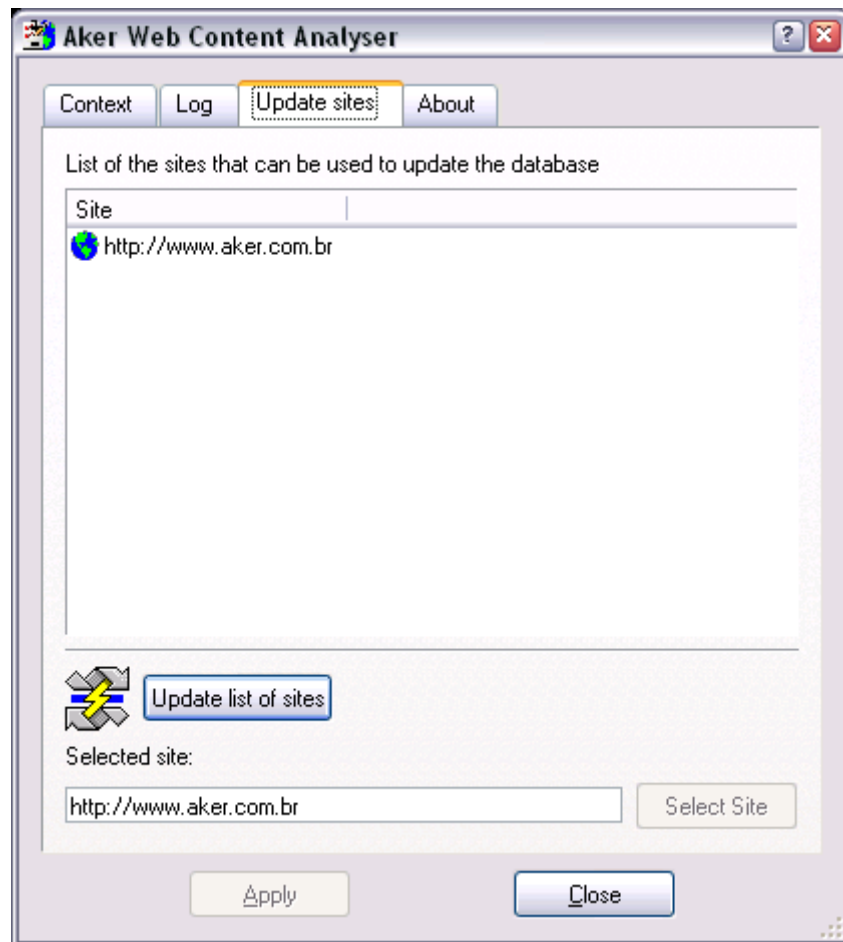
The **Erase** button, located in the toolbar allows the exclusion of all entries inside the log.

The **Save** button, located in the toolbar allows the saving of the log in a text format file. By clicking on it, a window asking for the filename to save the log will be displayed.

The option **Use event viewer**, if checked, will send the log messages to the Windows event viewer.

The description of all Aker URL Analyser log messages can be found in the [Appendix A](#).

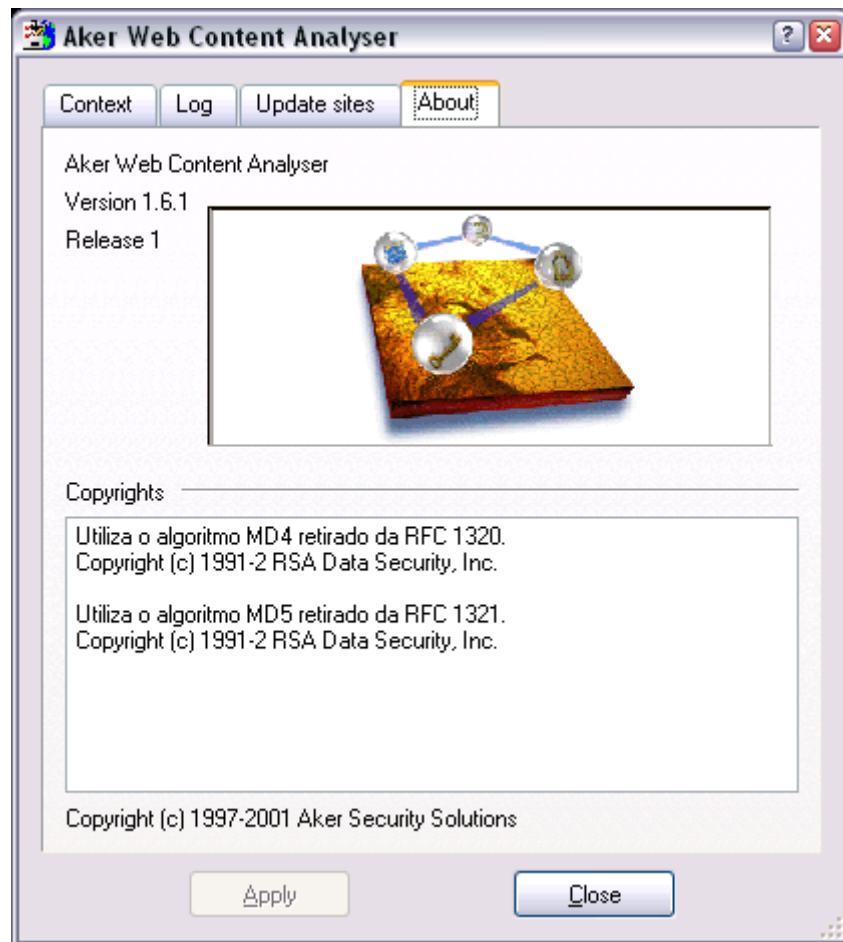
Update Sites



In order to minimize the traffic to Aker Security Solutions servers, the URLs database can be distributed to other Aker's partners. As soon as these sites start to function, the ***List of Sites for Database Update*** will automatically become available for the user that, will be able to choose the one with smallest delay, just by selecting the desired site and clicking on the ***Select Site*** button.

A forced update of the list can be done at anytime, by clicking on the **Update Sites List** button.

About



This is a merely informative tab, useful to acquire some information about the URL Analyser. Some of the useful pieces of information are the product version and release.

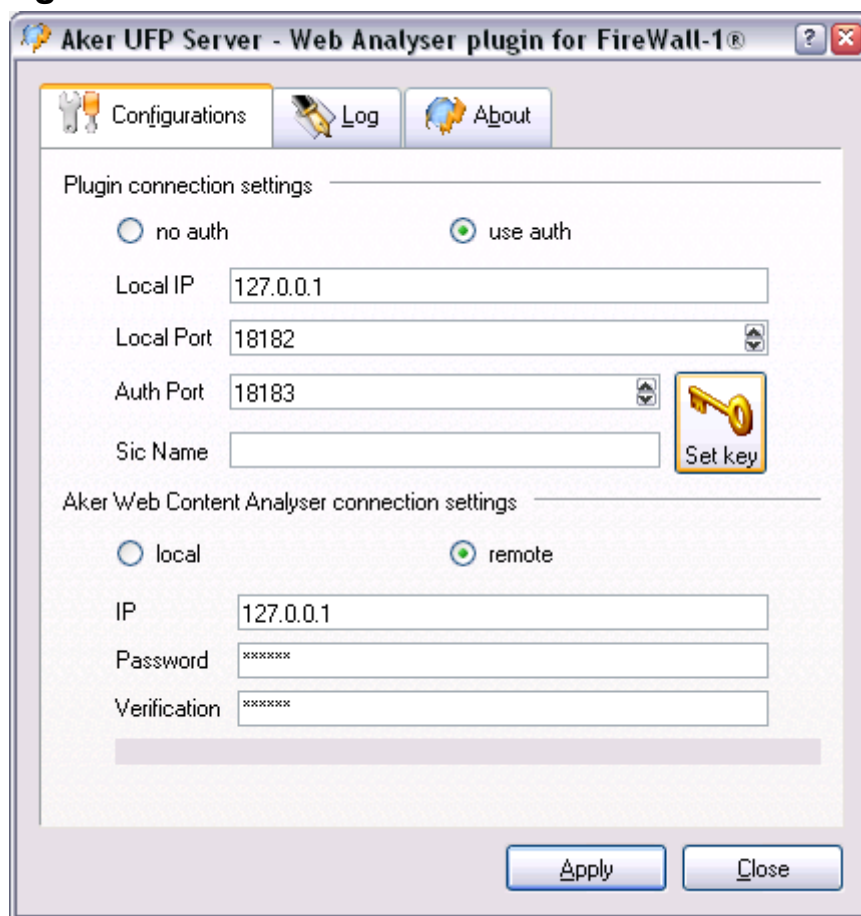
3-0 Using the Firewall - 1 Plugin

In this section the Aker Web Analyzer Firewall-1 Plugin usage will be explained

3-1 Introduction

The Firewall-1 plugin works as a gateway between Checkpoint Firewall - 1 and Aker Web Context Analyzer. To perform its tasks, it must be configured so that it can connect to both parties.

3-2 Configuration



The window above allows for configuring both the Plugin - Firewall-1 and the Plugin - Web Analyzer connections.

- Connecting to the Firewall-1:

The network traffic between the plugin and the Checkpoint Firewall 1 can be unprotected (**no auth**) or protected by digital authentication and cryptography (**use auth**).

The plugin will wait for Firewall-1 connections on the address **Local IP** and port

Local port.

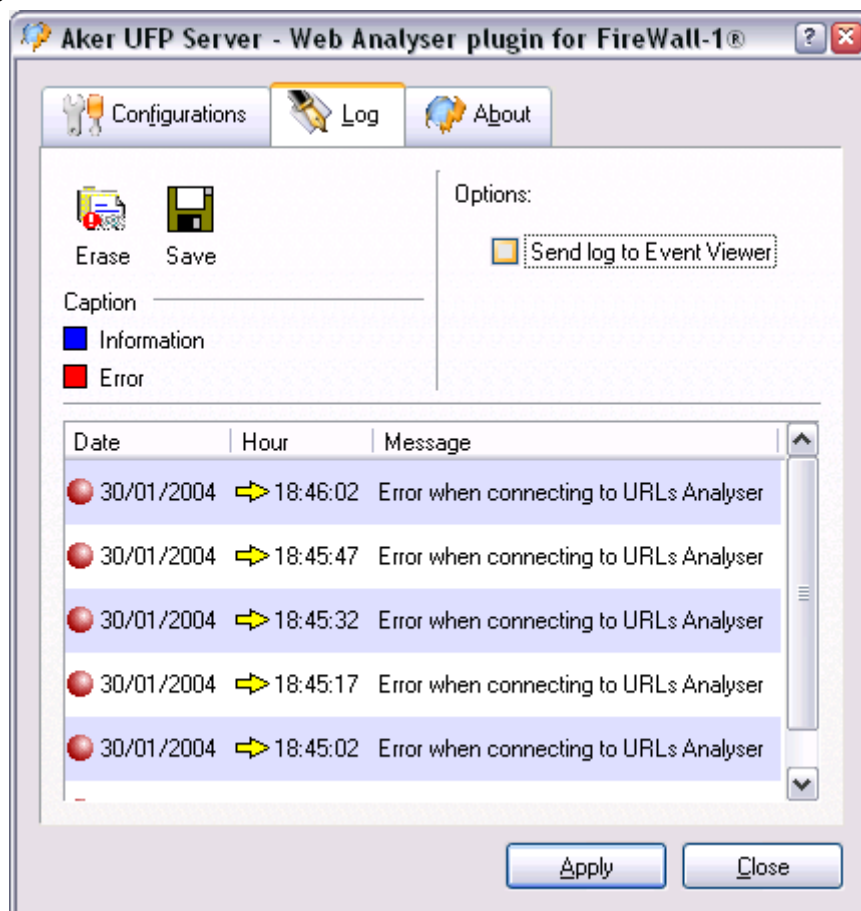
If you wish to use the authenticated mode, you must also configure **Auth Port** (port for authentication) and **Sic Name**. The shared secret must be entered in the dialog invoked by the *Set key* button.

All parameters must be set to same values both on the plugin (windows above) and in the Firewall - 1 configuration.

Connecting to the Aker Web Content Analyzer

There are two options for this connection: **local** (only on Linux O.S.), which uses a fast method called *local sockets* to connect to the Aker Web Context Analyzer running on the same computer as the plugin; and **remote**, which uses a TCP/IP connection to connect to a plugin which can be installed on a separated machine. The second option uses a strong encrypted and authenticated channel to protected all data.

3-3 Logs



This windows shows the system relevant events. You can then choose to **Save** them (in a text file) and to have the plugin use directly the system log facilities (**Event Viewer**, in Windows OSES and **Syslog** in Linux ones).

4-0 Using the Squid plugin

In this chapter the Aker Web Control for Squid usage and configuration will be discussed

4-1 Introduction

The Aker Web Control for Squid is a product which enables a powerful, profile-based filtering scheme to run alongside the Squid caching abilities. According to its configuration file, Squid will run several plugin, instances and have the URLs analyzed by it.

4-2 Squid Configurations

There are four Squid configuration directives which are relevant to the Aker Web Control for Squid:

- `cache_effective_user` - Defines the O.S. user Squid uses to run its processes. This user should be a non-privileged one, and must be also set in the plugin GUI.
- `cache_effective_group` - Defines the O.S. user Squid uses to run its processes. This user should be a non-privileged one, and must be also set in the plugin GUI.
- `redirect_program` - Tells Squid which program it should use to filter the user accesses requests. This should point to the file:

```
/usr/local/squid-urld/squid-urld
```

- `redirect_children` - Defines how many plugin process instances Squid will run. This number is the maximum number of simultaneous requests being analyzed at any given time. It is recommended to set it to a value never less than 5 and to increment it slowly, in order to avoid severe O.S. resource overuse.
- `auth_param basic program` - Tells Squid which program it should use to authenticate users. This should point to the file:

```
/usr/local/squid-urld/squid_auth /etc/passwd
```

- `auth_param basic children` - Defines how many squid_auth process instances Squid will run. This number is the maximum number of simultaneous requests being analyzed at any given time. It is recommended to set it to a value never less than 5 and to increment it slowly, in order to avoid severe O.S. resource overuse.

4-3 Plugin configurations

The screenshot shows a window titled "Aker Web Analyser plugin for Squid" with a yellow title bar. Below the title bar is a menu bar with icons and labels for "Configuration", "Profiles", "Users", "Groups", "Networks", and "About". The "Configuration" tab is active. The main area contains several sections:

- Log file**: A text field containing "/var/log/squid-urld.log".
- Default profile**: A dropdown menu showing "default".
- Default URL**: A text field containing "http://www.aker.com.br/squid-urld-block.html".
- Squid effective group and user**: Two dropdown menus. The "User" dropdown shows "nobody" and the "Group" dropdown shows "nogroup".
- Aker Web Analyser location**: A section with radio buttons for "local" (selected) and "remote". Below are five text fields labeled "Primary IP", "First backup", "Second backup", "Password", and "Verification", all of which are currently empty.

At the bottom right, there are two buttons: "Apply" and "Close".

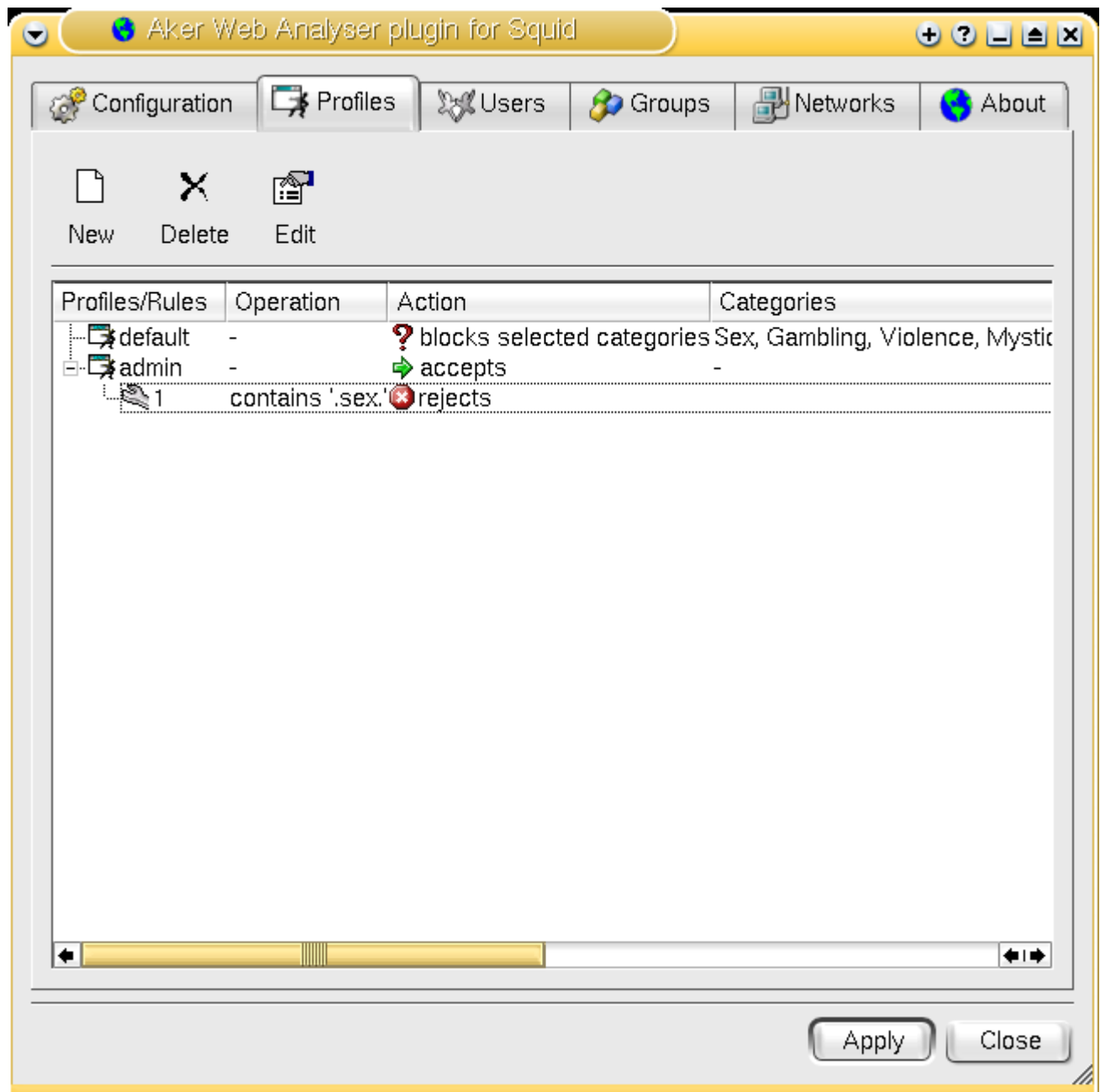
- **Log file:** This field points to a file to which the plugin will write relevant facts logs, such as errors connecting to the Web Context Analyzer itself. Please remember this file will be written by a process running with the Squid effective user and group ids.
- **Default profile:** If the plugin cannot find a specific profile for a request looking in its *users*, *groups* and *IP addresses* tables, it will use this one.
- **Default URL:** When the plugin decides a given user request for a specific URL should be blocked, it will redirect the user's browser to some other URL. This redirection URL can be defined either in the rule, the profile or, if none of these

is filled, the default URL. Moreover, some special character sequences can be inserted in the URL, in order to produce a more sophisticated web page:

Special sequence	replaced by
%%	'%' character
%u	Blocked URL
%s	User who tried to access a forbidden page
%i	IP address where the forbidden page request came from
%m	HTTP method used (GET, PUT, ...)
%d	Web server (FQDN) to which the desired request was directed

- **Squid effective group and User:** Should contain the same values entered in the Squid configuration file `cache_effective_user` and `cache_effective_group` lines.
- **Aker Web Analyzer location:** Tells the plugin how to communicate with the Aker Web Context Analyzer program:
 - Using **local** sockets: This method only works when running the plugin on the same machine as the Web Content Analyzer itself
 - Using TCP/IP **remote** sockets: This option will make the plugin open a authenticated and encrypted TCP/IP connection to the Web Content Analyzer, which can then be installed on a different machine.

4-4 Access Profiles and Rules



An access profile is made of an ordered rule set and a default action. The profiles have a hierarchic organization, i.e., a profile created in an inferior level will possess the rules of the profile of superior level to which it is subordinated. It is important to emphasize that the rules can only be modified on the profile they were created.

The rules are split into two distinct components:

1. **Search component:** A small text and a search operation which defines how to search the text in the client-given URL.
2. **Action component:** There are four possible actions when a the rule search components matches the URL:
 - **Allows:** Lets the URL access proceed
 - **Rejects:** Does not allow the URL access to proceed. Instead redirects the user's browser to the give redirection URL.

- **Blocks selected categories:** Classifies the URL access and, if it points to a site of any of the selected categories, rejects it using the redirection URL. Otherwise, lets it proceed.
- **Allows selected categories:** Classifies the URL access and, if it points to a site of any of the selected categories, lets it proceed. Otherwise, rejects it using the redirection URL.

In the profile, a redirection URL and a default action (if none of the rules match) are also specified. Therefore, the redirection URL used is determined in the following order:

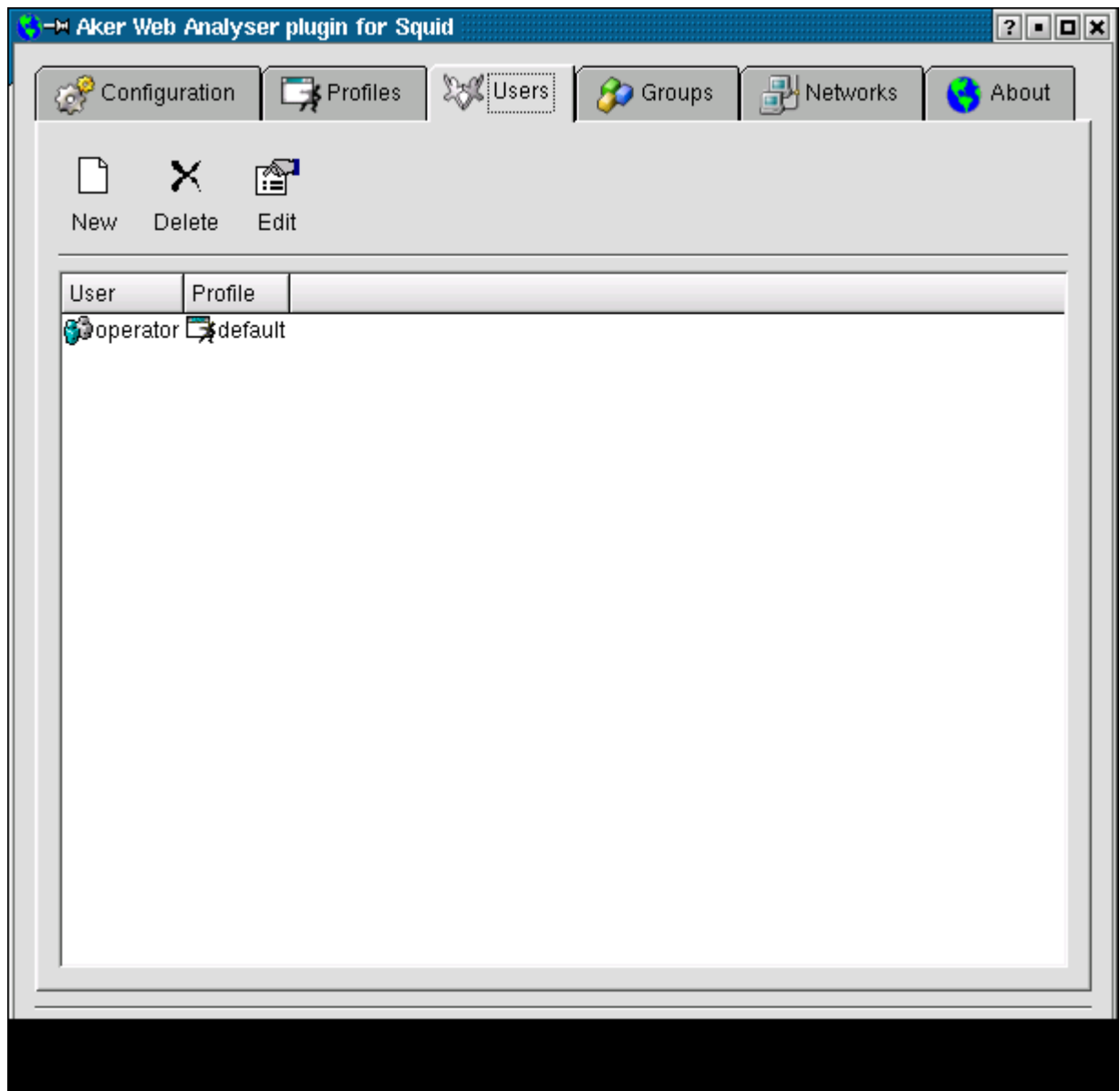
1. The rule-given, if it is not blank
2. The profile-given, if it is not blank
3. The default one, if both the rule and the profile ones are blank

4-5 Profile selection

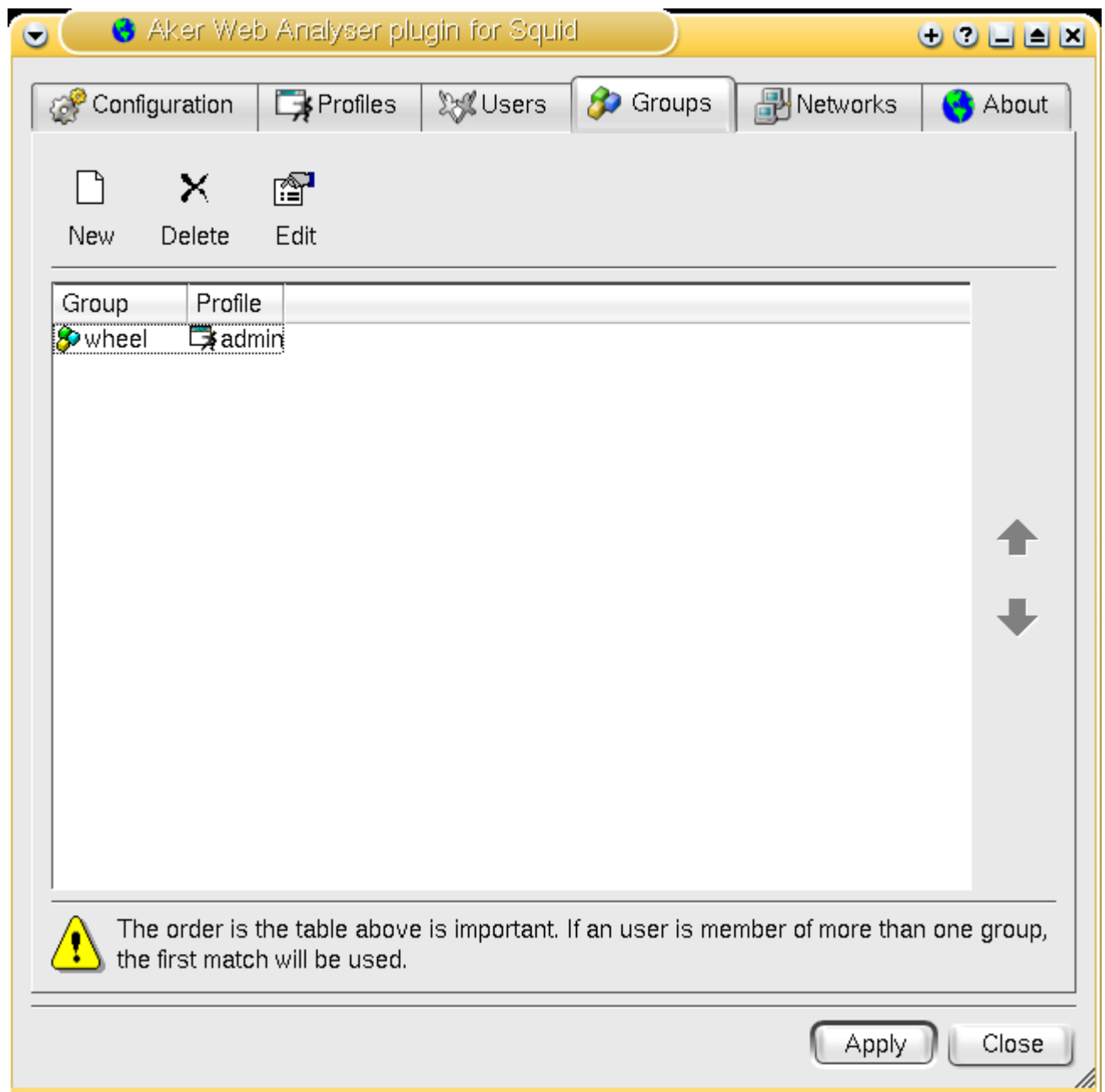
Once the access profiles are defined, the plugin must be configured to know which one of them to use for each request, analyzing the request's characteristics. The following request data can be used for this task, in this order:

1. **User name**
2. **O.S. group(s) to which the username belongs**
3. **User's browser IP address**

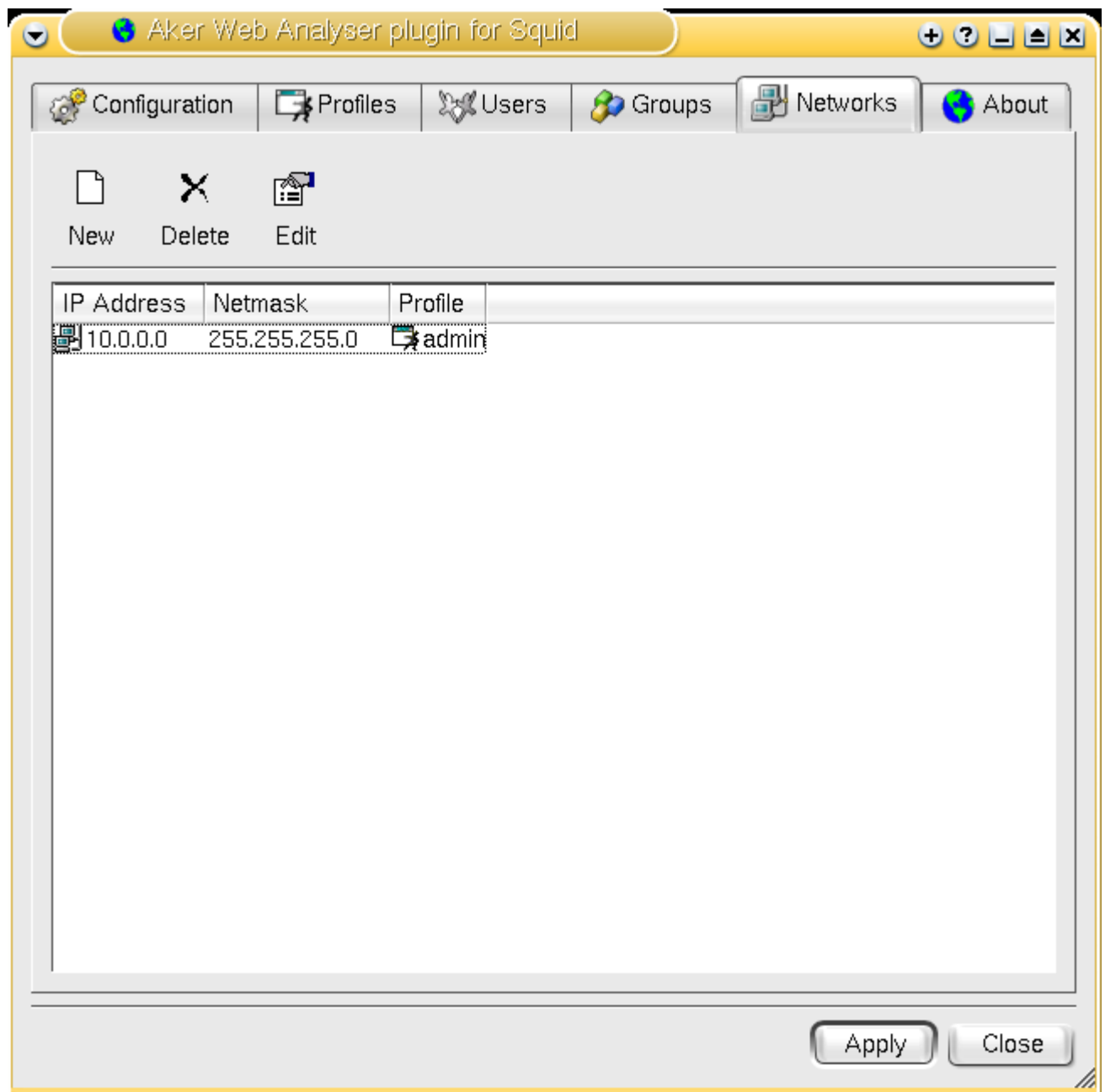
The following screens are used to set up the profile selection rules.



When editing or including a user-profile association in this list, it is possible either to choose a O.S. user from the combo-box or to write directly a arbitrary one. User names are determined by the Squid program itself, using another class of plugins.



Likewise, the groups can be chosen from the O.S. ones or directly entered by the administrator. On the other hand, the Squid program will not inform the plugin about the user's groups. These will be determined by the O.S. in the computer where the plugin is running.



If a profile cannot be determined from the user name or the user groups, the plugin will try to choose one based on the user's IP address.

5-0 Using the ISA Server plugin

In this chapter the Aker Web Control for ISA Server usage and configuration will be discussed

5-1 Introduction

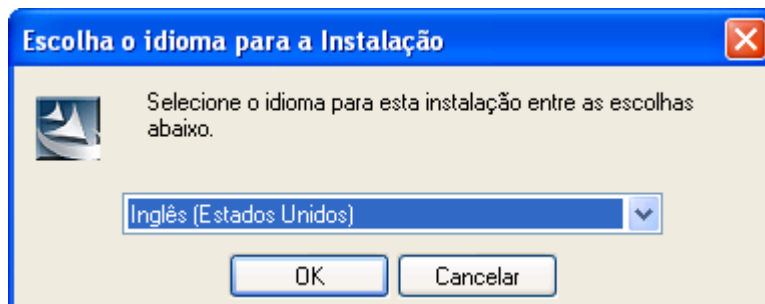
The Aker Web Control for ISA Server is a product which enables a powerful, profile-based filtering scheme to run alongside the ISA Server caching abilities.

5-2 Installing the plugin

The installation procedure is quite straightforward. Just follow the steps bellow:

1. Click the **Start** menu button
2. Select the **Run** option
3. When asked about which program to run, type `aker_web_control_isa.exe`

The following window will be displayed, choose the desired language for the installation and click on the *OK* button



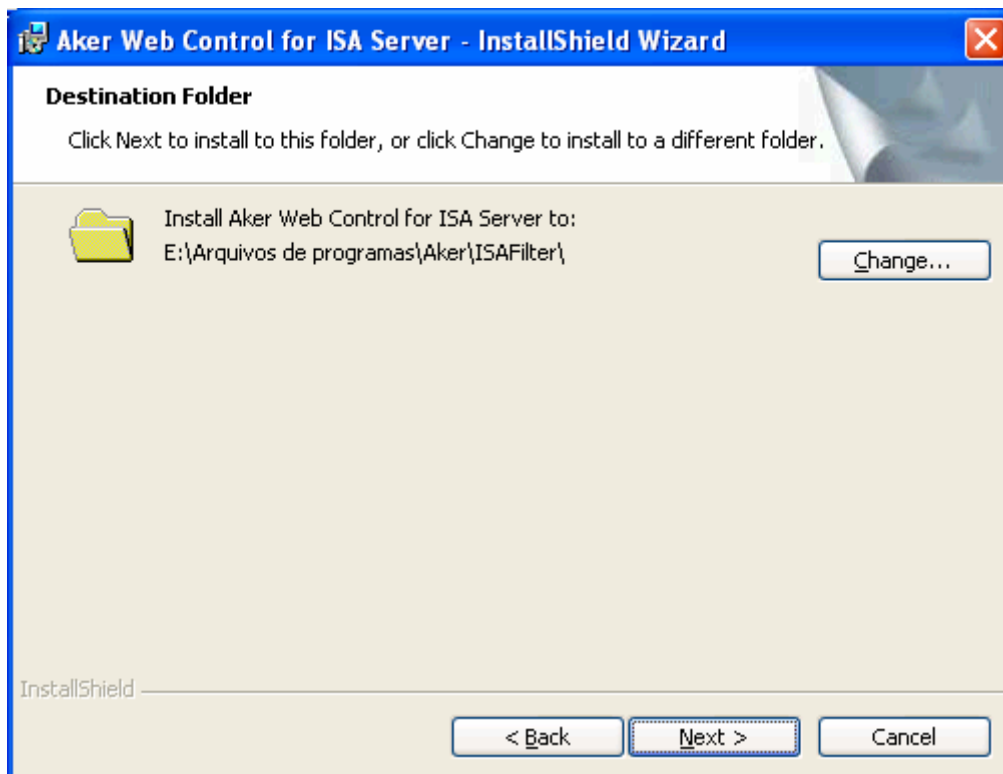
The window bellow will be displayed, being necessary to click on the *Next* button to proceed with the installation:



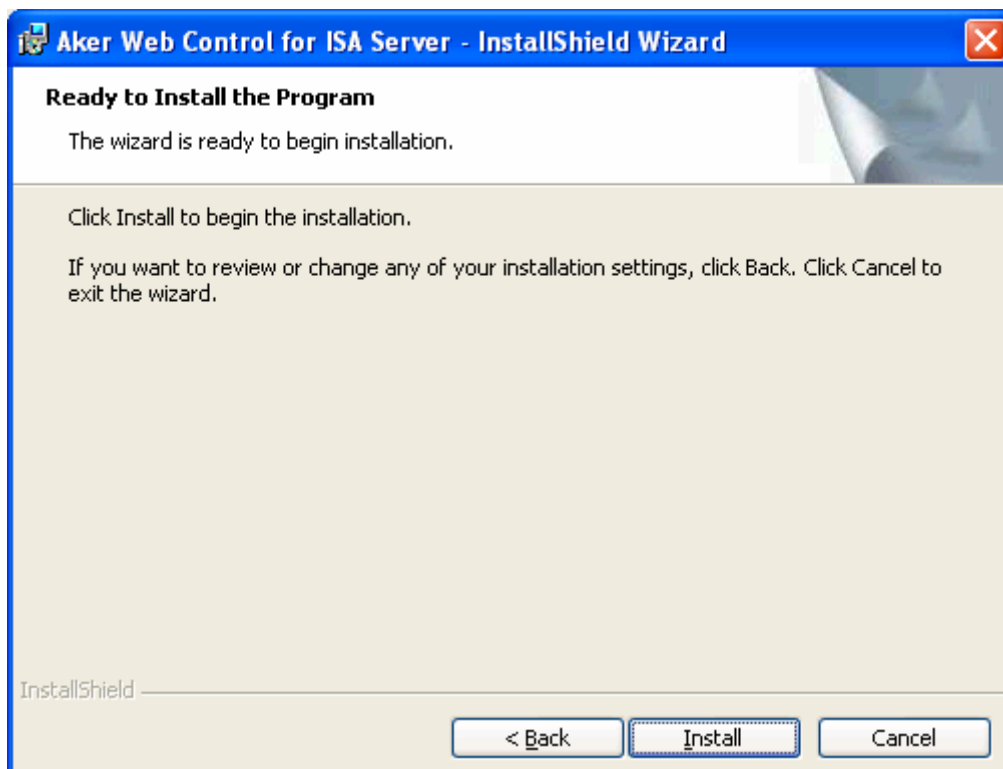
The next screen shows the license agreement. In order to have the installation proceed, select the option **I accept the terms in the license agreement**, after carefully reading it. If you don't accept, the installation will abort.



Choose the installation folder.



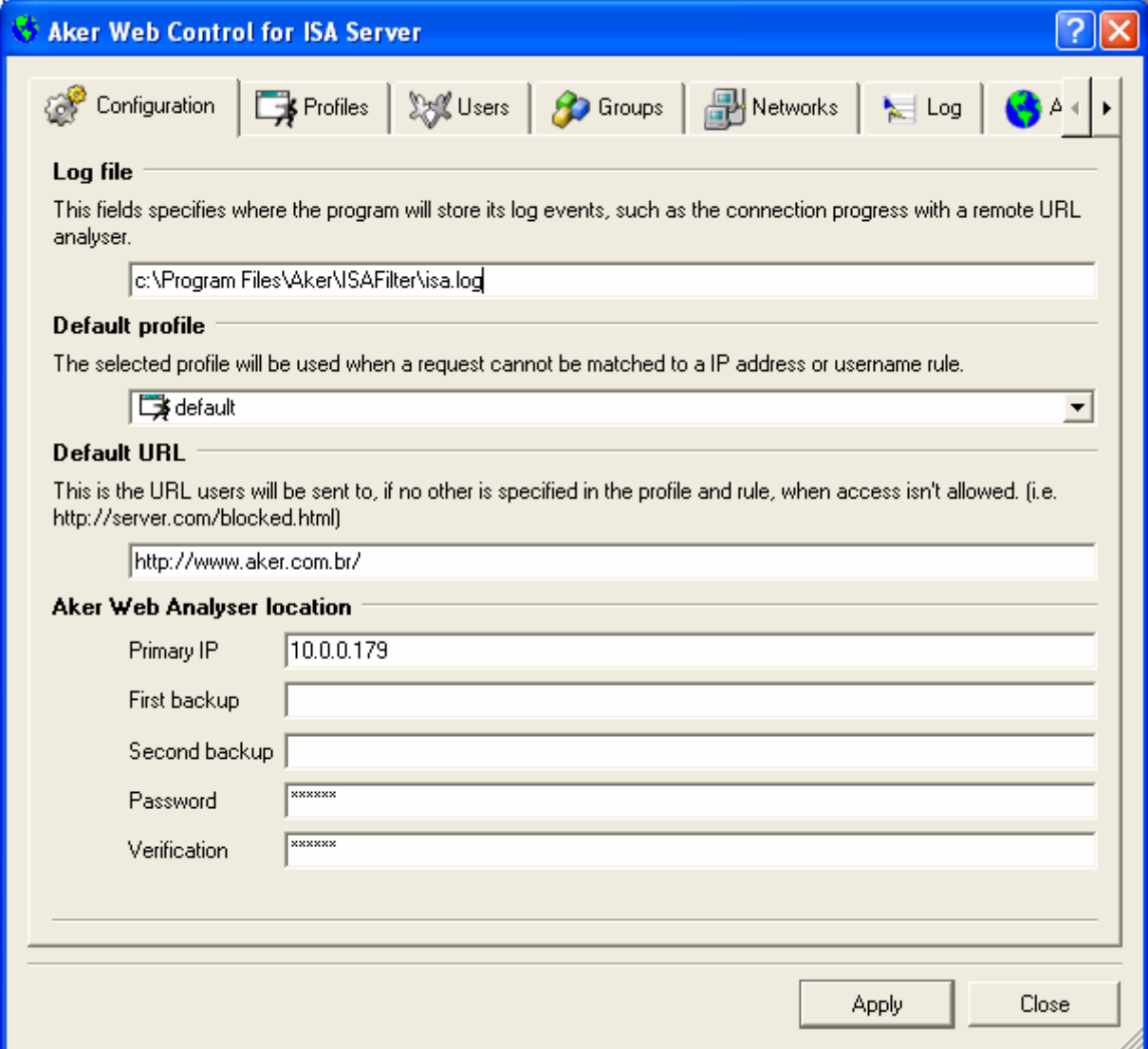
Press *Install* to have the program installed, according to your previous choices.



5-3 ISA Server Configurations

After installing the plugin you can activate/deactivate the filter by accessing the option **Servers and Arrays->[server name]->Extensions->Web Filters** on the **ISA Management** program.

5-4 Plugin configurations



The screenshot shows the 'Aker Web Control for ISA Server' configuration window. It has a blue title bar and a menu bar with icons for Configuration, Profiles, Users, Groups, Networks, Log, and a globe icon. The main area contains several sections:

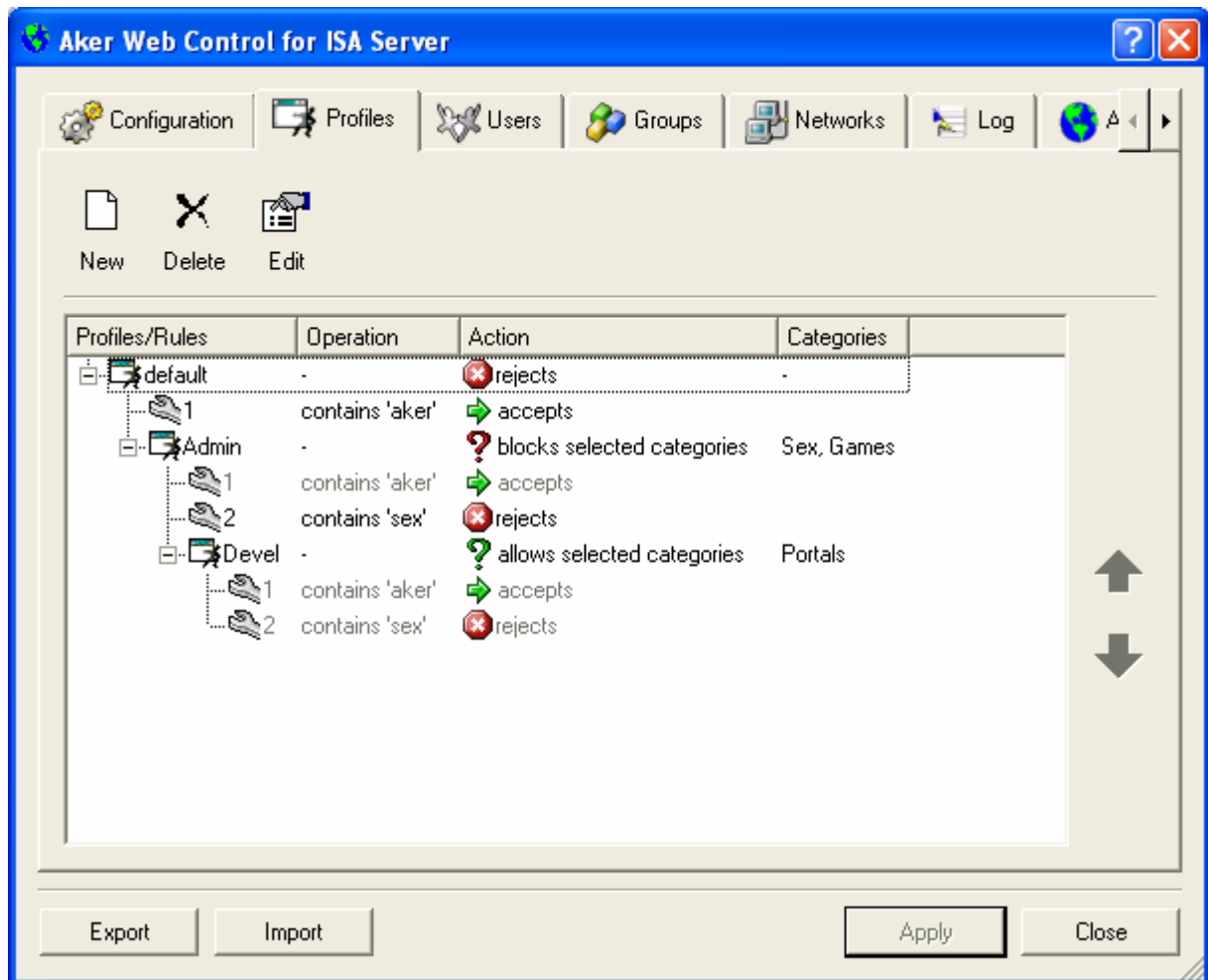
- Log file:** A text box containing 'c:\Program Files\Aker\ISAFilter\isa.log'. A description below states: 'This fields specifies where the program will store its log events, such as the connection progress with a remote URL analyser.'
- Default profile:** A dropdown menu showing 'default'. A description below states: 'The selected profile will be used when a request cannot be matched to a IP address or username rule.'
- Default URL:** A text box containing 'http://www.aker.com.br/'. A description below states: 'This is the URL users will be sent to, if no other is specified in the profile and rule, when access isn't allowed. (i.e. http://server.com/blocked.html)'
- Aker Web Analyser location:** A group of text boxes for 'Primary IP' (10.0.0.179), 'First backup', 'Second backup', 'Password' (masked with '*****'), and 'Verification' (masked with '*****').

At the bottom right, there are 'Apply' and 'Close' buttons.

- **Log file:** This fields points to a file to which the plugin will write relevant facts logs, such as errors connecting to the Web Context Analyzer itself.
- **Default profile:** If the plugin cannot find a specific profile for a request looking in its *users*, *groups* and *IP addresses* tables, it will use this one.
- **Default URL:** When the plugin decides a given user request for a specific URL should be blocked, it will redirect the user's browser to some other URL. This redirection URL can be defined either in the rule, the profile or, if none of these is filled, the default URL. Moreover, some special character sequences can be inserted in the URL, in order to produce a more sofisticated web page:

Special sequence	replaced by
%%	'%' character
%u	Blocked URL
%s	User who tried to access a forbidden page
%i	IP address where the forbidden page request came from
%d	Web server (FQDN) to which the desired request was directed

5-5 Access Profiles and Rules



An access profile is made of an ordered rule set and a default action. The profiles have a hierarchic organization, i.e., a profile created in an inferior level will possess the rules of the profile of superior level to which it is subordinated. It is important to emphasize that the rules can only be modified on the profile they were created.

The rules are split into two distinct components:

1. **Search component:** A small text and a search operation which defines how to search the text in the client-given URL.
2. **Action component:** There are four possible actions when a the rule search components matches the URL:
 - o **Allows:** Lets the URL access proceed
 - o **Rejects:** Does not allow the URL access to proceed. Instead redirects the user's browser to the given redirection URL.

- **Blocks selected categories:** Classifies the URL access and, if it points to a site of any of the selected categories, rejects it using the redirection URL. Otherwise, lets it proceed.
- **Allows selected categories:** Classifies the URL access and, if it points to a site of any of the selected categories, lets it proceed. Otherwise, rejects it using the redirection URL.

In the profile, a redirection URL and a default action (if none of the rules match) are also specified. Therefore, the redirection URL used is determined in the following order:

1. The rule-given, if it is not blank
2. The profile-given, if it is not blank
3. The default one, if both the rule and the profile ones are blank

In the URL field can be specified a redirection to a local file using an URL of the form "file://complete_path_to_file". In case of a HTML file all images must be stored in the directory "<install_dir>\images\" and loaded on code like the example below:

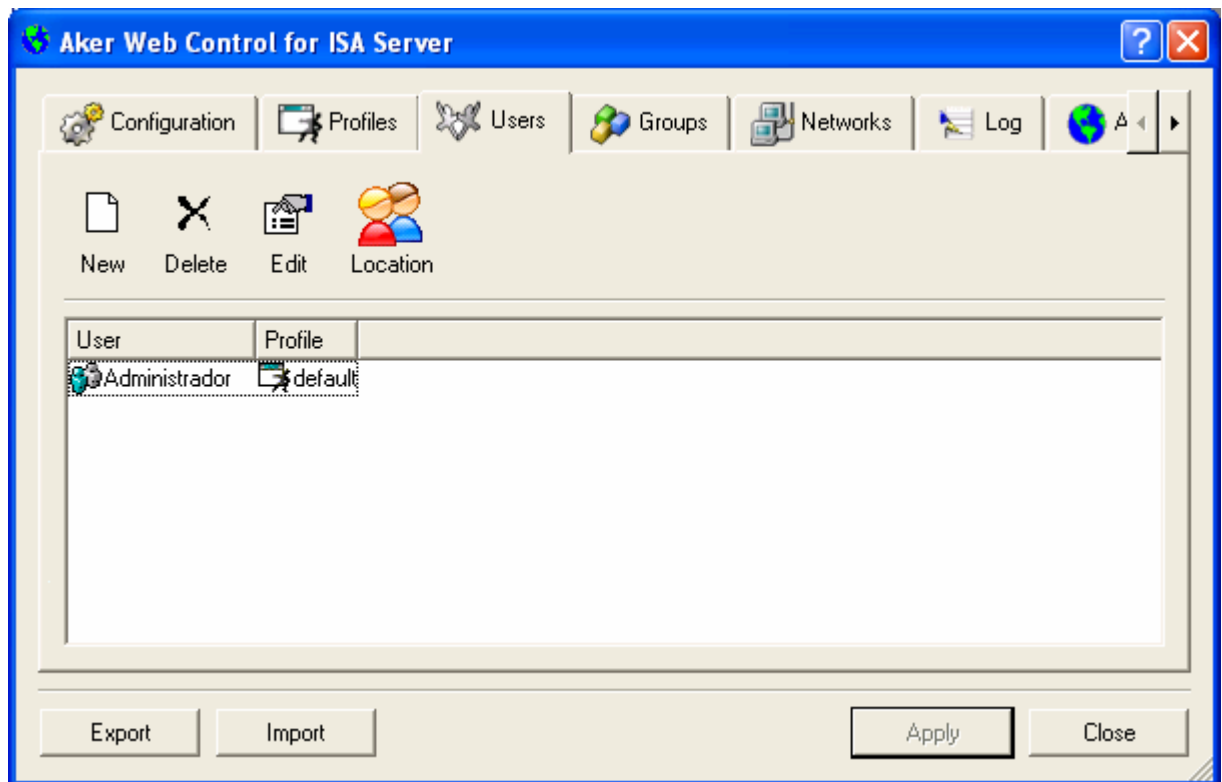
IMG SRC = "http://10.10.10.10/example.gif" (in case of a server accessible by IP 10.10.10.10)

5-6 Profile selection

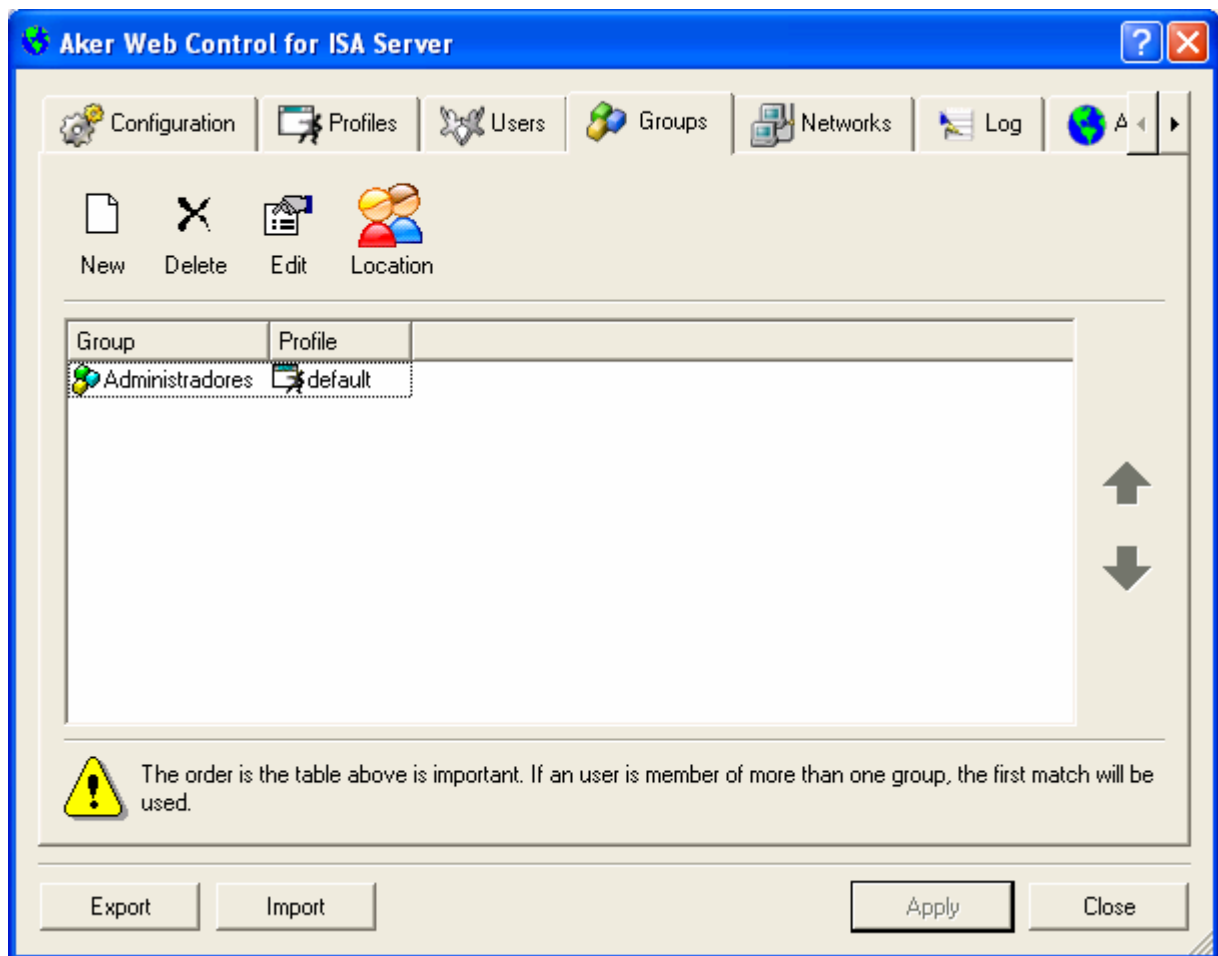
Once the access profiles are defined, the plugin must be configured to know which one of them to use for each request, analyzing the request's characteristics. The following request data can be used for this task, in this order:

1. **User name**
2. **O.S. group(s) to which the username belongs**
3. **User's browser IP address**

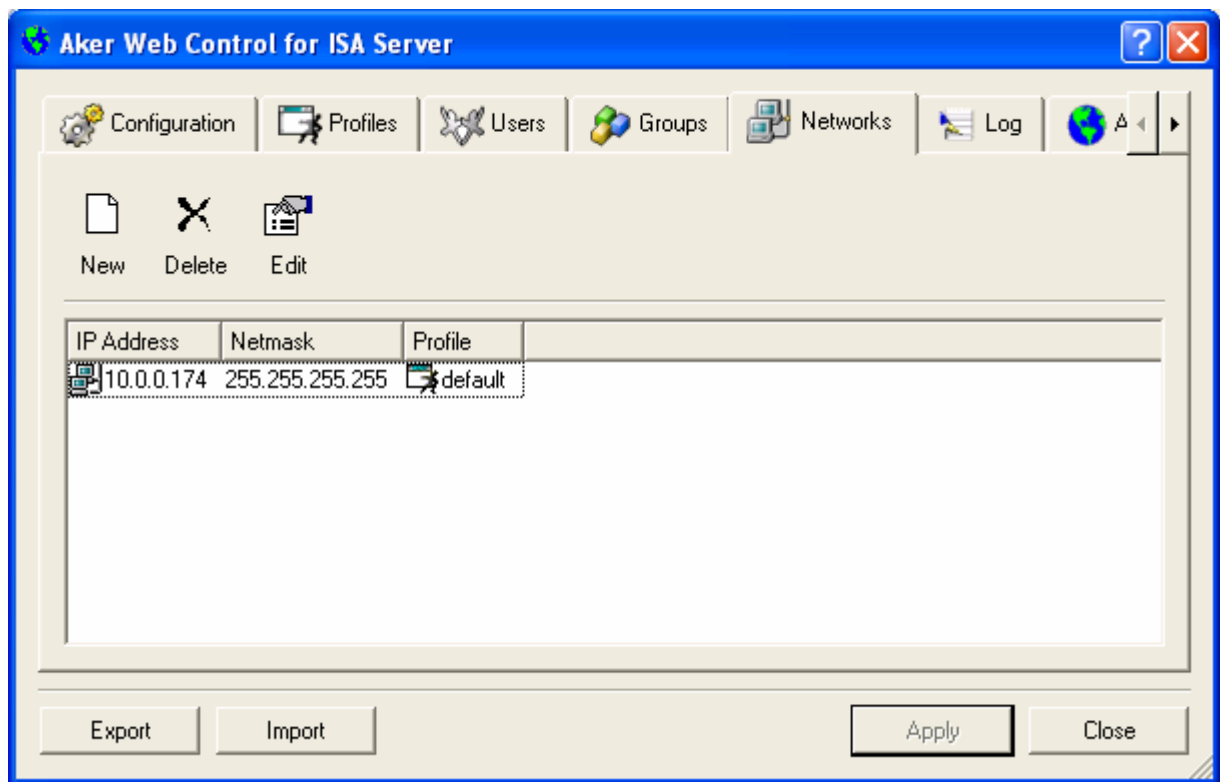
The following screens are used to set up the profile selection rules.



When editing or including a user-profile association in this list, it is possible either to choose an O.S. user from the combo-box, from an authentication agent or to write directly an arbitrary one. User names are determined by the server and depend on the authentication scheme used.



Likewise, the groups can be chosen from the O.S. ones, from an agent or directly entered by the administrator. On the other hand, the ISA Server program will not inform the plugin about the user's groups. These will be determined by the O.S. in the computer where the plugin is running or the authentication agent used.



If a profile cannot be determined from the user name or the user groups, the plugin will try to choose one based on the user's IP address.

Appendix A - Log Messages

Bellow are displayed all the messages that can appear in Aker URL Analyser. Whenever presented, they will be complemented by a register containing additional information about the event.

- **Socket creation error**

This message indicates that the analyser was not able to create the socket that was required for its functioning in the TCP/IP stack. Check if the TCP/IP protocol is installed and functioning.

- **Bind error**

This message indicates that the URL analyser was not able to associate its socket with the required port for its communication with the firewalls. Check if there is any other program using the same port.

- **Accept error**

Internal error in Winsocks protocol. Check if the TCP/IP protocol is correctly installed and functioning.

- **Data receive error**

This message indicates that problems occurred when receiving data from the firewall. Check the physical connection (cables, network adapters, hubs, etc) between the two machines.

- **Firewall closed the connection**

The connection with the firewall was unexpectedly closed. It can occur when the administrator restarts the firewall.

- **Communication authentication with Firewall**

The analyser could correctly authenticate a firewall that established a connection. The IP address of the firewall will be shown in the log message.

- **Attempt of connection from undefined Firewall**

The analyser received an attempt of a connection from an unregistered firewall, and because of that, refused it. To accept connections from a firewall, it is necessary to register it in the *Context* > *Firewalls* window.

- **Select error**

Internal error in Winsocks protocol. Check if the TCP/IP stack is correctly installed and functioning.

- **Data send error**

This message indicates that problems occurred when sending data to the firewall. Check the physical connection (cables, network adapters, hubs, etc) between the two machines.

- **Reestablishing Firewall connection**

This message indicates that one of the registered firewalls is reestablishing a connection with the URL analyser.

- **Firewall connection established successfully**

This message indicates the entire connection process has successfully been established.

- **Shutting down connections with Firewalls**

This message indicates that the firewalls using the URL analyser have been disconnected.

- **HTTP proxy authentication error**

The URL analyser could not update the user database due to a problem when connecting to the network proxy. Click on the Options button and check if the password and name are correctly written.

- **Site with no category**

The site is not registered in Aker URL Analyser database.

- **Site with undefined category**

The database is compromised. Please contact Aker Security Solutions technical support and notify the problem.

- **Sex site**

The URL is classified as containing sex content.

- **Hate speech site**

The URL is classified as containing offensive words and content.

- **Drugs or alcohol site**

The URL is classified as containing drugs or alcohol content.

- **Gambling site**

The URL is classified as containing gambling content.

- **Violence site**

The URL is classified as containing violence content.

- **Mysticism or astrology site**

The URL is classified as containing mysticism or astrology content.

- **Entertainment site**

The URL is classified as containing entertainment content.

- **Games site**

The URL is classified as containing electronic games content.

- **Hobbies site**

The URL is classified as containing hobbies content.

- **Investment site**

The URL is classified as containing financial or investment content.

- **Job search site**

The URL is classified as containing job searching content.

- **Travel site**

The URL is classified as containing traveling or tourism content.

- **Vehicles site**

The URL is classified as containing automobiles or motors content.

- **News site**

The URL is classified as containing news content.

- **Dating site**

The URL is classified as containing dating content.

- **Shopping site**

The URL is classified as containing shopping content.

- **Sports site**

The URL is classified as containing sports content.

- **Chat site**

The URL is classified as containing chat content.

- **Erotic site**

The URL is classified as containing erotic or nudism content.

- **Internet portal site**

The URL is classified as an Internet Portal.

- **Hackers site**

The URL is classified as containing hackers content.

- **Crimes or terrorism site**

The URL is classified as containing crimes or terrorism content.

- **MP3 or music site**

The URL is classified as containing music or MP3 content.

- **WebMail site**

The URL is classified as a WebMail.

- **Error while opening URL update file**

This message indicates that the database has been transferred, however the file could be compromised. Try to download the database again.

- **Invalid URL update file**

The analyser successfully transferred the database, however its format is incompatible. Try to download the database update again. If the problem persists, contact Aker Security Solutions technical support.

- **Error while reading URL update file**

The update file could be compromised. Try to download the update again.

- **Error while writing URL update file**

The content analyser cannot save the database file. Check if there is enough free disc space.

- **URL updated successfully**

The URL database was successfully updated. The additional message indicates the number of inserted, modified or deleted URLs since the last update.

- **Error while creating URLs update file**

The URL analyser could not save the database file. Check if there is enough free disc space and if the directory's writing permissions are correct.

- **Invalid URL**

The URL is incorrectly written. The correct format is
`http://www.sitename.domain.suffix`

- **Error while downloading URLs update file**

There has been a communication error with Aker Security Solutions server during the database transfer. Check if the update sites are correct.

- **URLs base file replacement failed**

The database replacement failed. Try to download the update or the entire database.

- **URLs base file replacement successful**

The database replacement was successfully achieved.

- **URLs base file corrupted**

The local database is compromised. Download the entire database, and if the problem persists, contact Aker Security Solutions technical support.

- **Updating daily URLs base file**

The URLs database updating is in progress.

- **File not available for download**

The URLs database for this date is not available for distribution yet. Try a new connection later.

- **Activation key not found**

The activation key is not in the specified directory. Execute the load procedures again.

- **Activation key expired**

The activation key has achieved the end of its usable time. Contact Aker Security Solutions to renew it.

- **Activation key will expire in a few days**

The activation key is close to its expiration time. The number of usable days is shown in the log. Contact Aker Security Solutions to renew it.

- **Proxy authentication failed**

The network proxy could be offline. Check the problem and try a new connection.

- **Firewall is already connected**

An already connected firewall is trying a new connection with the content analyser. It can occur if the firewall has been restarted.

During usual conditions, the URL analyser detects the new connection and closes the old one. If any problem occurs, just restart the service.

Appendix B - Copyrights and Disclaimers

In this appendix are listed the *disclaimers* of thirds source codes used in Aker URL Analyzer. These disclaimers are only applicable for the explicitly mentioned parts of the program, and not for Aker URL Analyzer as a whole. They are mentioned here as determined by their developers:

MD4 Algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD4 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

MD5 Algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

