

# KinderGate Parental Control

## Administrator Manual

## Table of Contents

<b>KinderGate Parental Control</b> .....	<b>1</b>
<b>Administrator Manual</b> .....	<b>1</b>
<b>System Requirements</b> .....	<b>3</b>
<b>KinderGate Parental Control Installation</b> .....	<b>3</b>
<b>KinderGate Parental Control Update and Removal</b> .....	<b>4</b>
<b>KinderGate Parental Control Registration</b> .....	<b>4</b>
<b>KinderGate Parental Control Access Management</b> .....	<b>4</b>
Website Category Filtering.....	5
Address Filtering.....	6
Internet Access Schedule.....	7
Content Filtering.....	8
Advanced Filtering Rules.....	9
<b>Special Traffic Filtering Methods</b> .....	<b>10</b>
Contextual Advertising Filter.....	10
Secure Search.....	11
Secure Search.....	12
Morphological Analysis.....	12
Instant Messages Recording.....	16
<b>Cancel Access Denial</b> .....	<b>17</b>
<b>KinderGate Parental Control Statistics</b> .....	<b>18</b>
<b>Password Recovery</b> .....	<b>20</b>
<b>Appendix</b> .....	<b>22</b>
ICQ client denial.....	22
Social networks access denial.....	24
Hide pictures on a specific website.....	25
Deny Web-mail category and allow access to mail.yahoo.com as an exception.....	27

KinderGate Parental Control is a tool that allows parents to control how their children use Internet resources. The product features URL filtering, website category filtering and Internet access schedules. The program has a user-friendly interface and provides online statistics in graphs and charts.

## System Requirements

Recommended system requirements for KinderGate Parental Control include a Windows XP/Vista/Windows 7 PC with a broadband or Dial-Up Internet connection. The program needs at least 512 MB RAM and 20 MB free disk space to run properly. Free disk space requirements generally depend on how long KinderGate Parental Control has been collecting statistics in its own database.

## KinderGate Parental Control Installation

To install KinderGate Parental Control, run the installer when you are in a user profile with administrator rights. Installation Wizard will complete all the required actions, such as unpack the files, create an additional system service for KinderGate Parental Control and install two extra drivers. Current network connections will be terminated after installation of a network driver. KinderGate Parental Control will launch automatically upon installation. No system reboot is required.

KinderGate Parental Control will be installed by default to folder %Program Files%\Entensys\KinderGate (further referred to as %KinderGate%). KinderGate Parental Control configuration files (ugpc.xml) and statistics database file (ugpc.fdb) are placed in the same folder. Configuration file can only be modified from KinderGate Parental Control Administrator Console. Application files are protected by the application's integrated file system driver.

Setting administrator password is an important step in the installation process. The password you set will be used to establish connection between the Administrator Console and KinderGate Parental Control service. Besides, you will be prompted for the password if you decide to uninstall the application. You can set the filtering level on the Settings page, and it may be later changed from Administrator Console.

### KinderGate Parental Control Update and Removal

To check for KinderGate Parental Control updates, click the “Check for Updates” button on “About” page in the Administrator Console. This will match the number of your installed version against the number of the latest version available on the vendor’s website. Checking for application updates will not automatically start the update process – it is only designed to advise an administrator of a new version’s release.

### KinderGate Parental Control Registration

When you first start the Administrator Console, the activation process will launch automatically. The activation wizard will help you obtain a demo or a full license key for your KinderGate Parental Control. The key request is sent to the vendor website (<http://www.entensys.com>) via the Internet over HTTPS protocol. This protocol must be enabled in your network settings to allow proper activation.

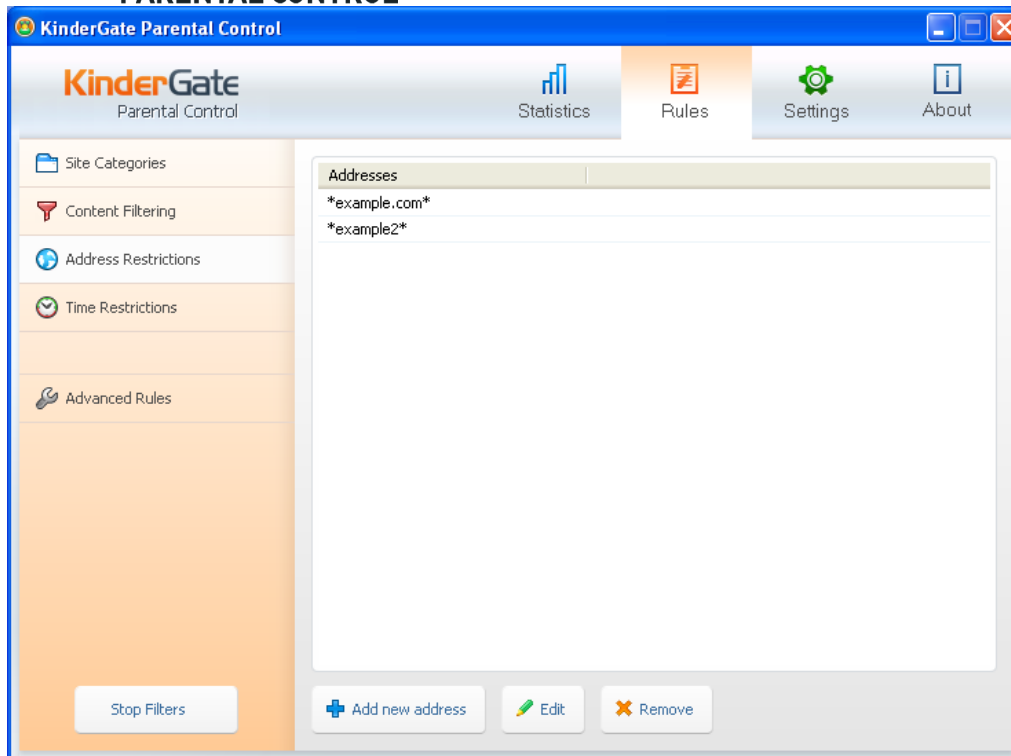
A temporary 30-day license key will be generated when you request a demo key. KinderGate Parental Control will stop filtering traffic after the demo key expires.

If you are requesting a full license key, the activation wizard will prompt you for a special pin code given to you with the program.

When activating the program, an administrator will also be prompted for a random registration name, some personal data and an Email address that will be used to send a new password to if the original KinderGate Parental Control password is lost.

### KinderGate Parental Control Access Management

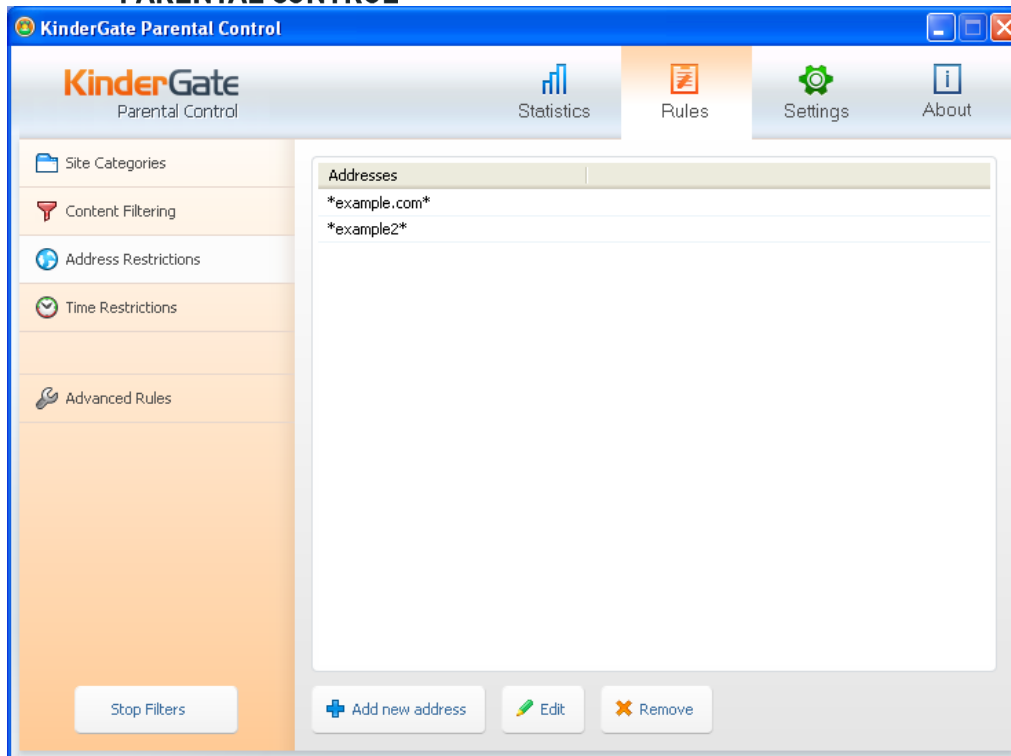
You may use KinderGate Parental Control to restrict or deny access to potentially dangerous or unwanted Internet resources. The Entensys URL Filtering solution integrated into the KinderGate product supports multiple filtering methods.



## Website Category Filtering

Select one of the preset filtering levels on the “Rules” page of KinderGate Parental Control console for easier administration. Each level will automatically deny access to preset website categories. You may disable category filtering if necessary.

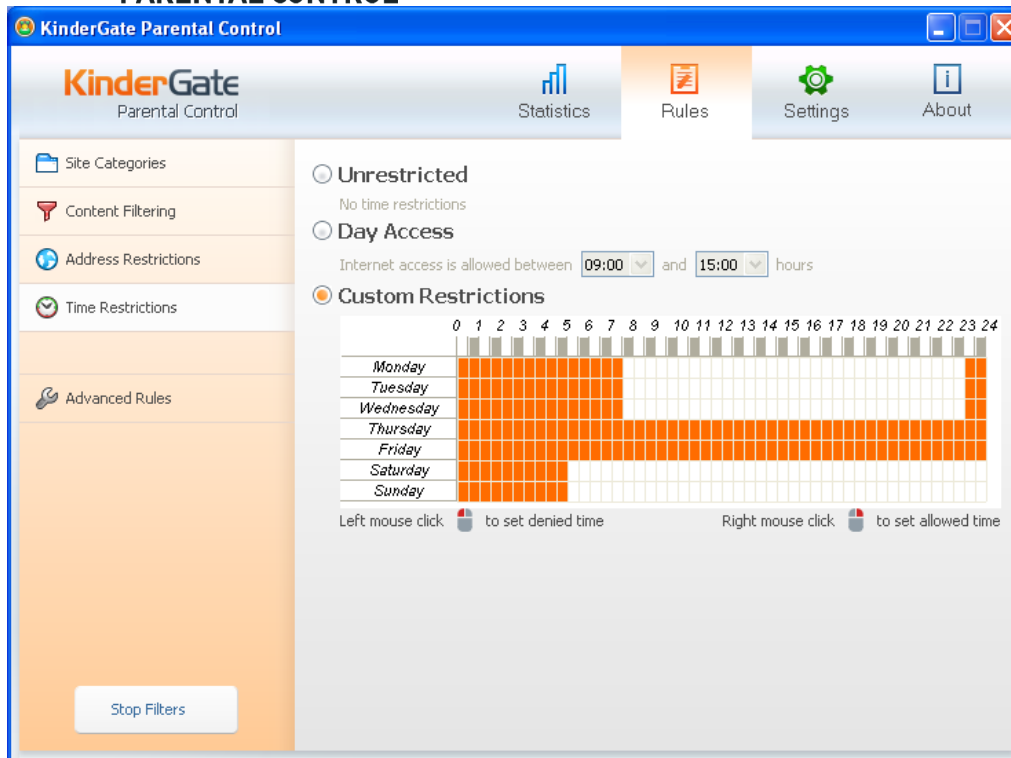
The browser window will display a KinderGate Parental Control message every time access to a website of a particular category is blocked.



## Address Filtering

In addition to category filtering, KinderGate Parental Control offers the address filtering feature. Banned addresses need to be listed on the “Address Restrictions” page of KinderGate Parental Control console. Each address may contain a special character (i.e., \* stands for random set of characters) at the beginning or the end of the line. Special characters inside the address line are not supported.

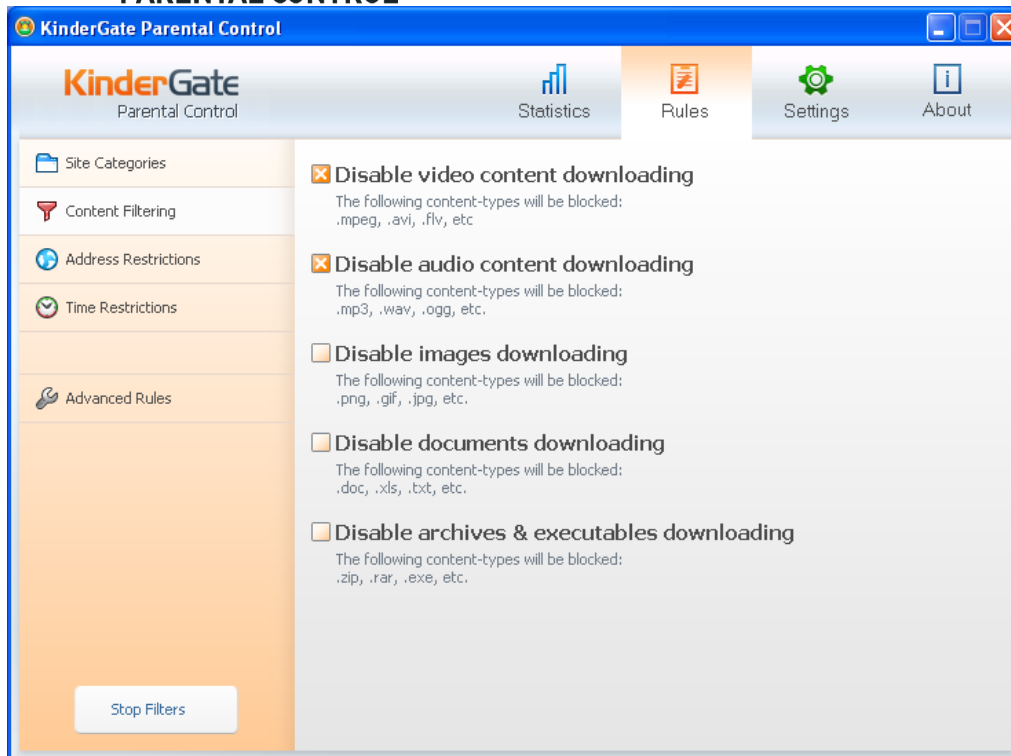
The browser window will display a KinderGate Parental Control message every time access to a website with address restriction is blocked.



## Internet Access Schedule

With KinderGate Parental Control, you may create Internet access schedules. By default, Internet access is allowed at all times, but you may select one of the available restriction options (“Day Schedule” or “Random Schedule”) on the “Scheduled Restrictions” page. The first option is used to set the exact time when Internet access is allowed each day. The second option allows setting random time periods on random days of the week.

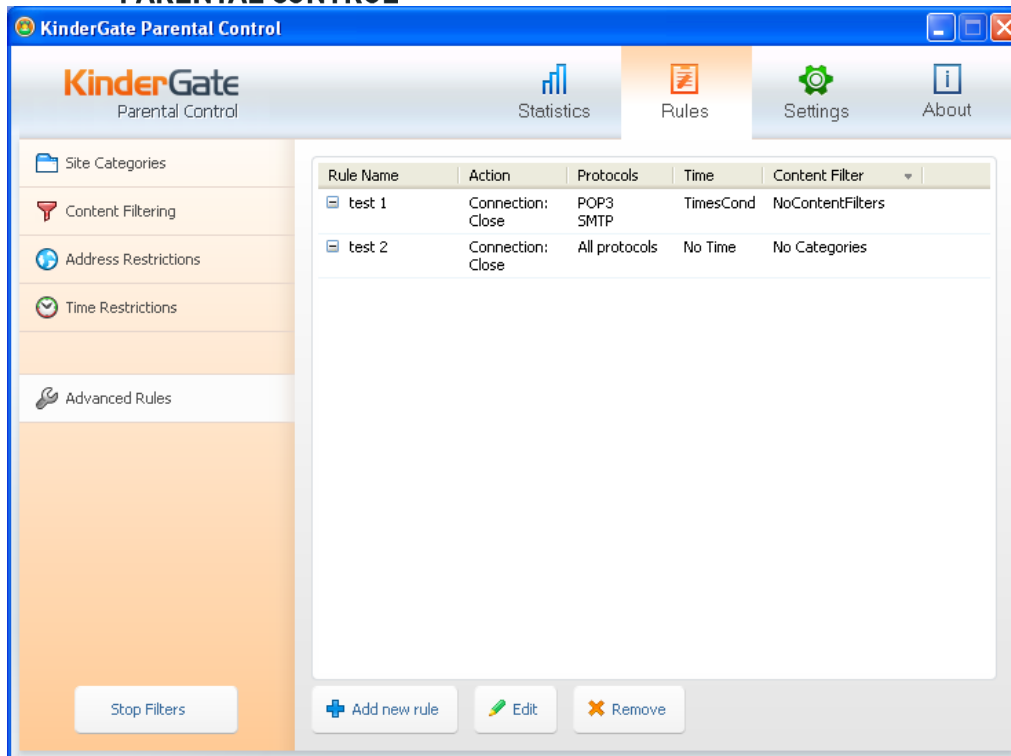
The length of online sessions is not monitored and, therefore, not subject to restrictions.



## Content Filtering

You may select one or more preset content download modes on the “Content Restrictions” page.

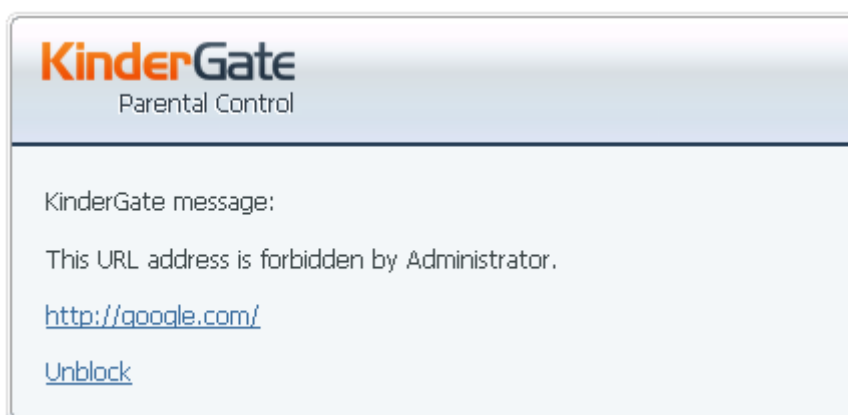
You can also configure the program to deny downloads of media files, executable files, archives and documents on the same page.



## Advanced Filtering Rules

In addition to preset filtering modes, KinderGate Parental Control offers advanced filtering features. You may create advanced filtering rules on the “Advanced Rules” page of KinderGate Parental Control console.

See the examples of advanced filtering rules in the Appendix.



## Special Traffic Filtering Methods

To achieve a more comprehensive traffic monitoring, version 1.1. has been augmented with special monitoring tools that allow blocking requests to search engines, such as google.com, yandex.ru, etc. These tools analyze website content to identify banned words and track the content of messages transmitted via messaging services, including ICQ and MSN, and popular social networks (facebook, vkontakte, odnoklassniki).

### **Contextual Advertising Filter**

This filter is based on the knowledge of basic parameters of online advertising, including banner dimensions, banner codes and special banner detection techniques. This method helps you block almost all advertising content on any website quickly and effectively and secures you from popup windows. Were you ever irritated by advertisements at file hosting sites such as letitbit and like?! If you were, enable this filter and you will never see any advertising or popup windows again.

The filter can only be enabled or disabled.

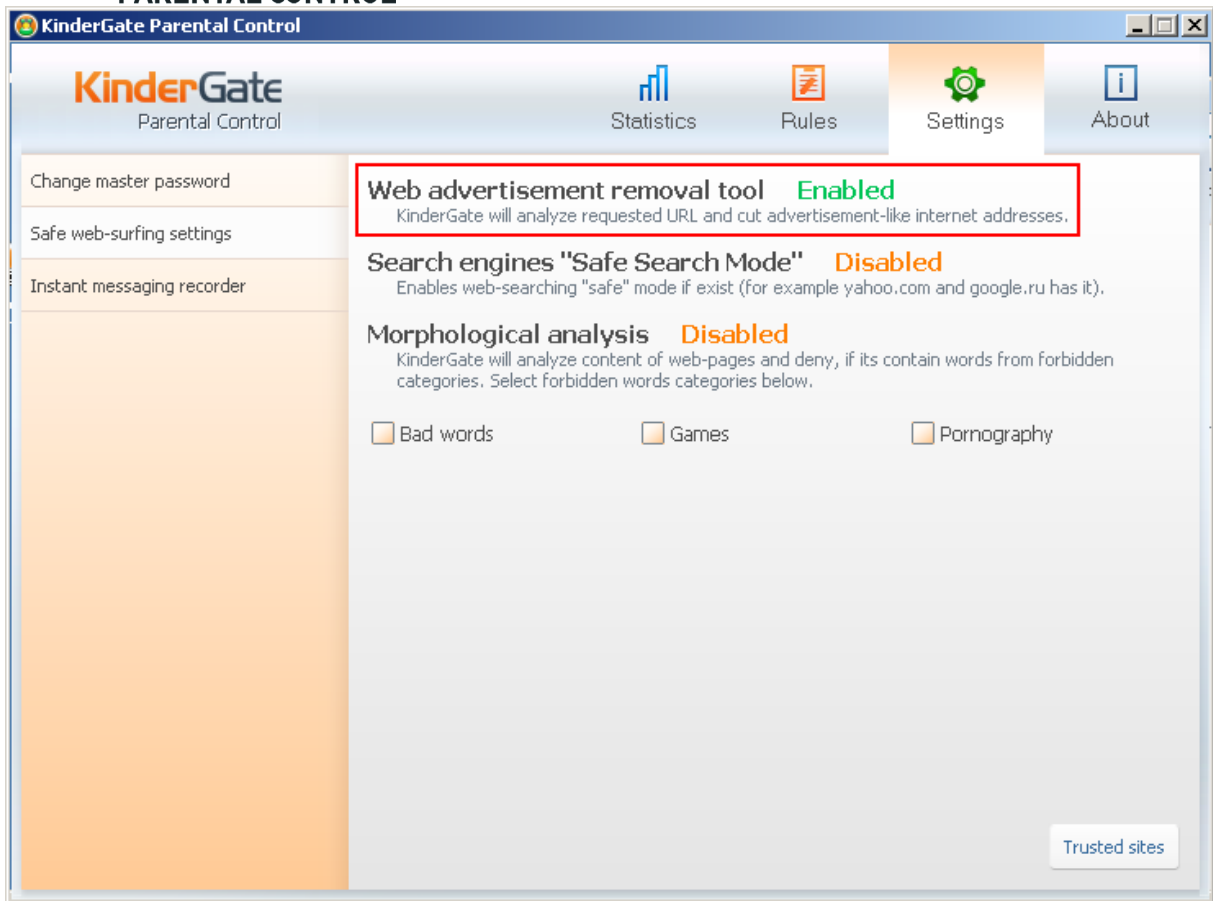


Fig. 6. Contextual Advertising Filter

## Secure Search

This setting can be used to enable or disable parental control filter for different search engines, including Google, Yandex and some others. When you enable Secure Search, the system will block requests for any prohibited content, such as porn or foul language. The tool does not only filter websites – it also denies access to pictures and video files. We recommend you to enable this setting as it does not impact your computer performance and is extremely effective.

## Secure Search

This setting can be used to enable or disable parental control filter for different search engines, including Google, Yandex and some others. When you enable Secure Search, the system will block requests for any prohibited content, such as porn or foul language. The tool does not only filter websites it also denies access to pictures and video files. We recommend you to enable this setting as it does not impact your computer performance and is extremely effective.

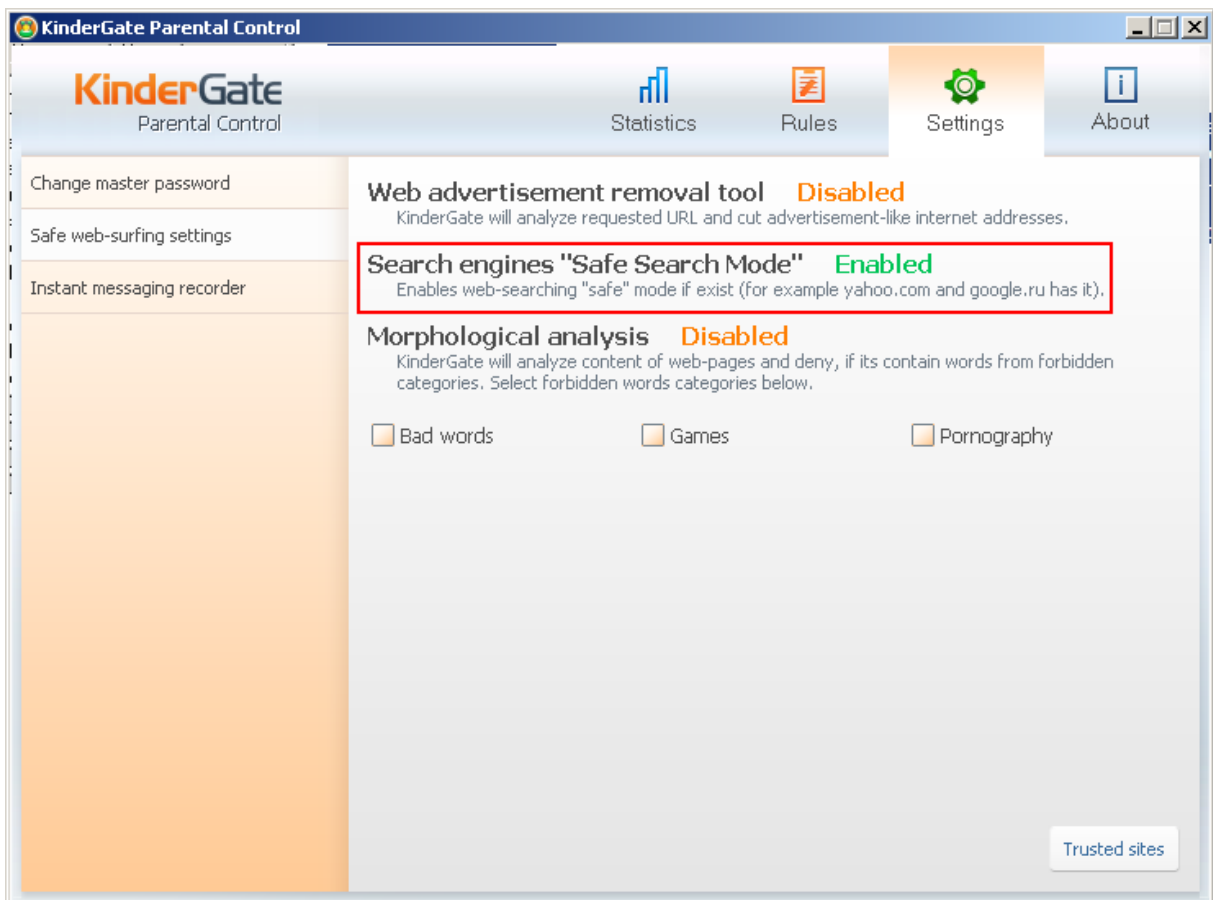


Fig. 7. Secure Search

## Morphological Analysis

Morphological analysis tool recognizes individual phrases in the content of websites and blocks access to the entire website if the analysis detects forbidden words in

such phrases. This tool can be very effective if other blocking tools cannot block a certain online resource or a group of resources with similar content.

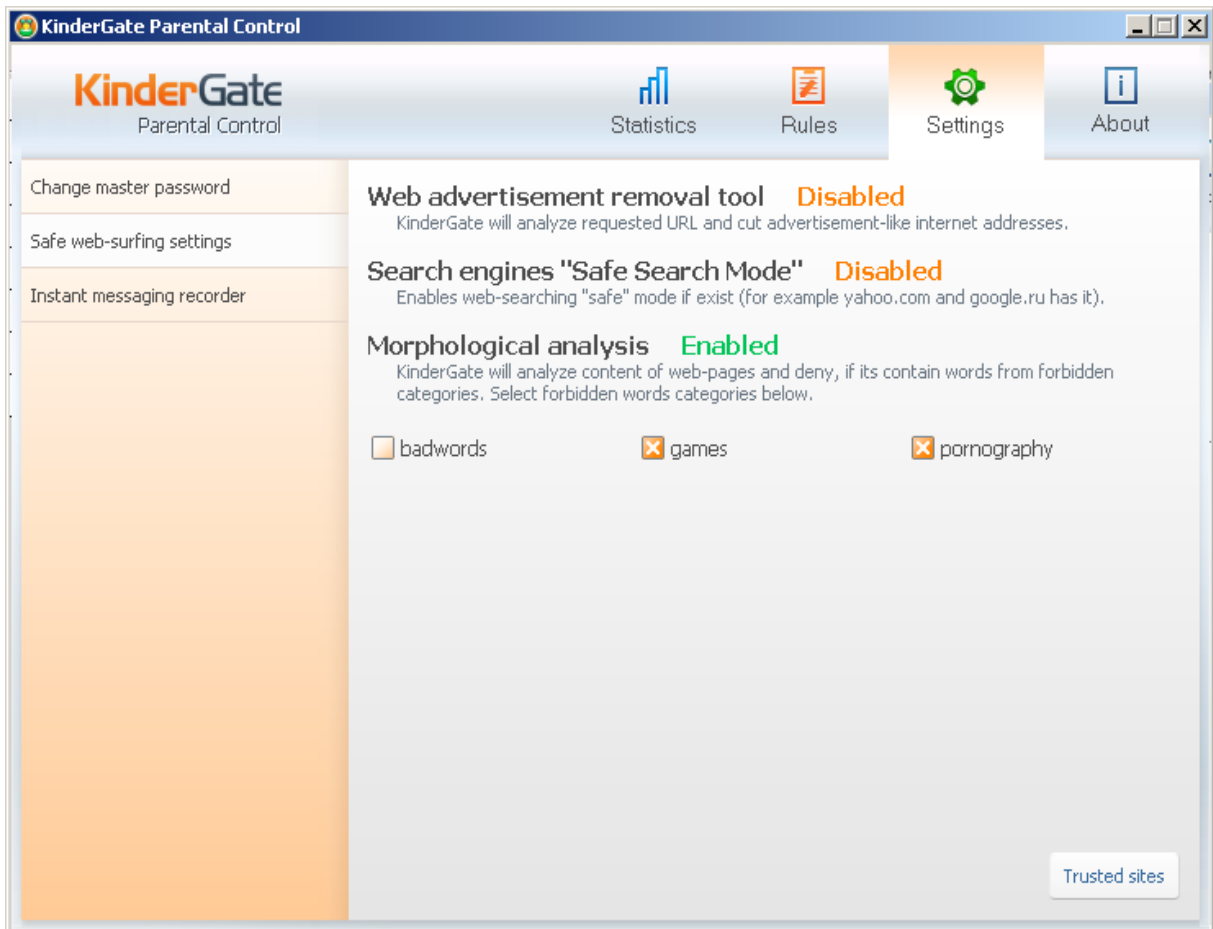


fig. 9 Morphological analysis

When the application was originally designed, developers did not enable prohibited words list editing capability in the morphological analysis component.

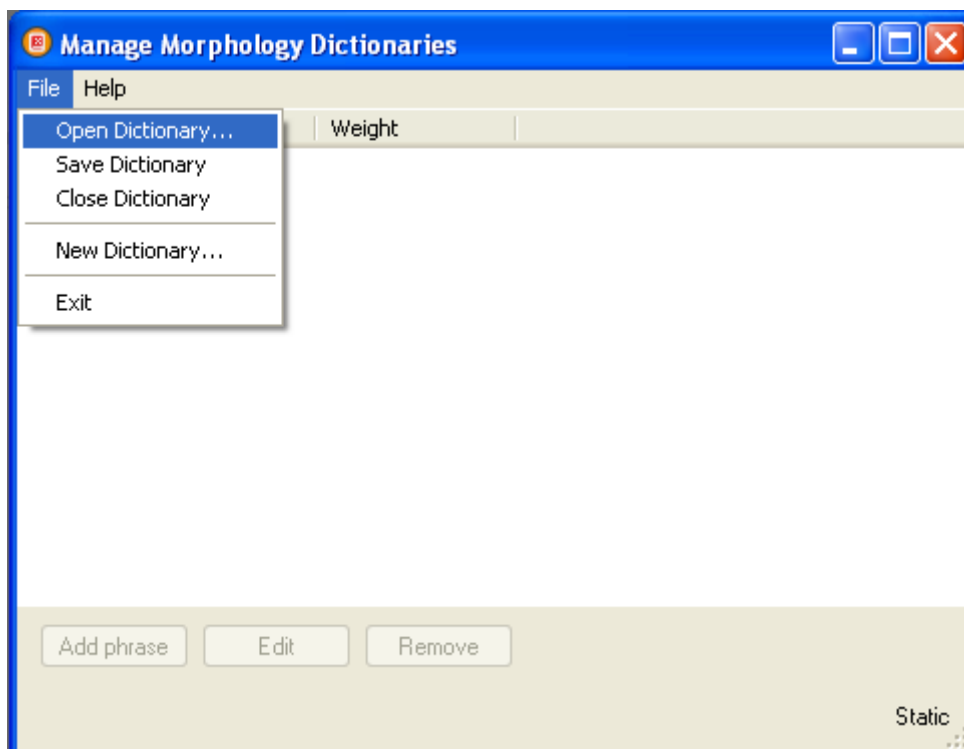
However, the need for an editing tool became obvious later. A special utility (**dictutil.exe**) was developed that can be used to edit the list of prohibited words. The application is installed in KinderGate folder: "C:\program files\entensys\kindergate" for 32-bit OS and "C:\program files (x86)\entensys\kindergate" for 64-bit OS. In Windows 7, you have to work in the OS as an administrator to launch the application.

When you have launched the utility, select the appropriate dictionary (File – Open Dictionary...) and edit it. In default configuration, access to the web page will be

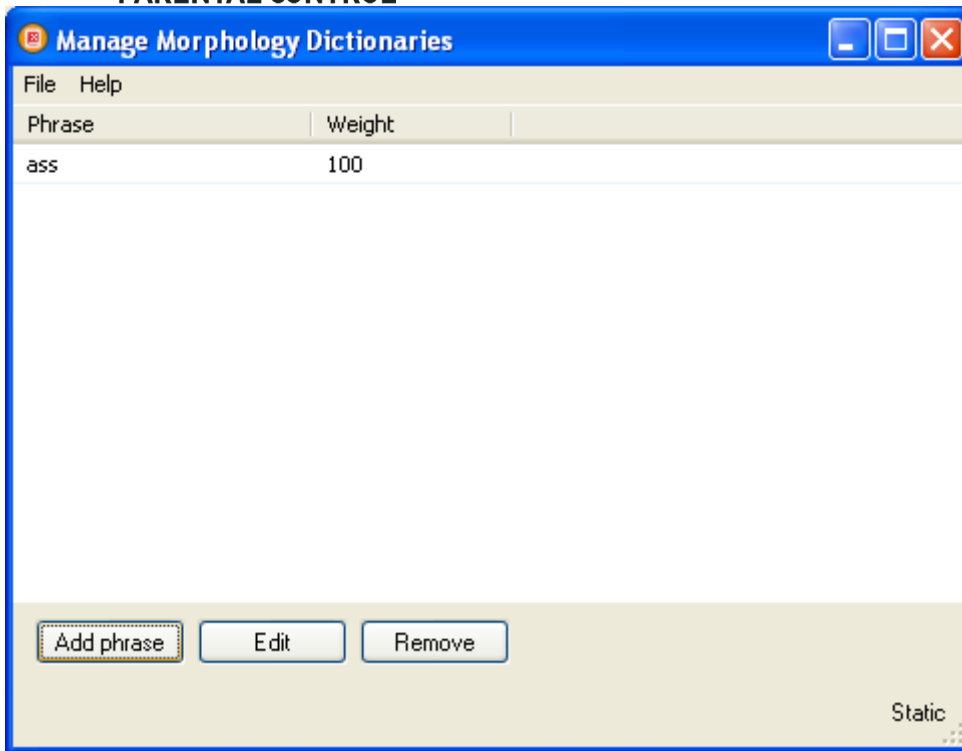
blocked if a word's weight on the page is 100. If you want the system to block access to a web page immediately when it sees an unwanted word, set the word's weight at 100. Please see illustrations below for explanations.

**Important!** Only Latin alphabet can be used to name new dictionaries! When you restart the service, your new dictionary will be added by the application in the "Web-surfing settings" page.

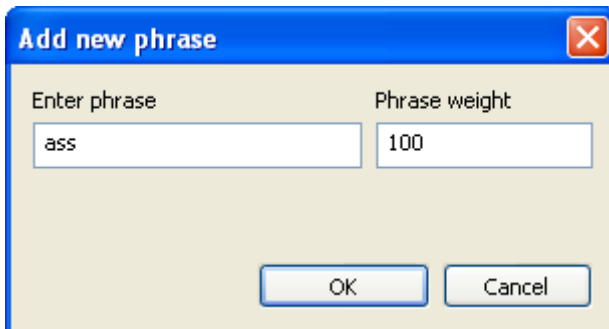
**Important!** Save changes after editing the dictionary (File – Save Dictionary...) and restart KinderGate service (Start – Control panel – Administration – Services - KinderGate Parent Control – right-click on the service name and select "restart"). The words you have added to the dictionary will not be blocked by the application.



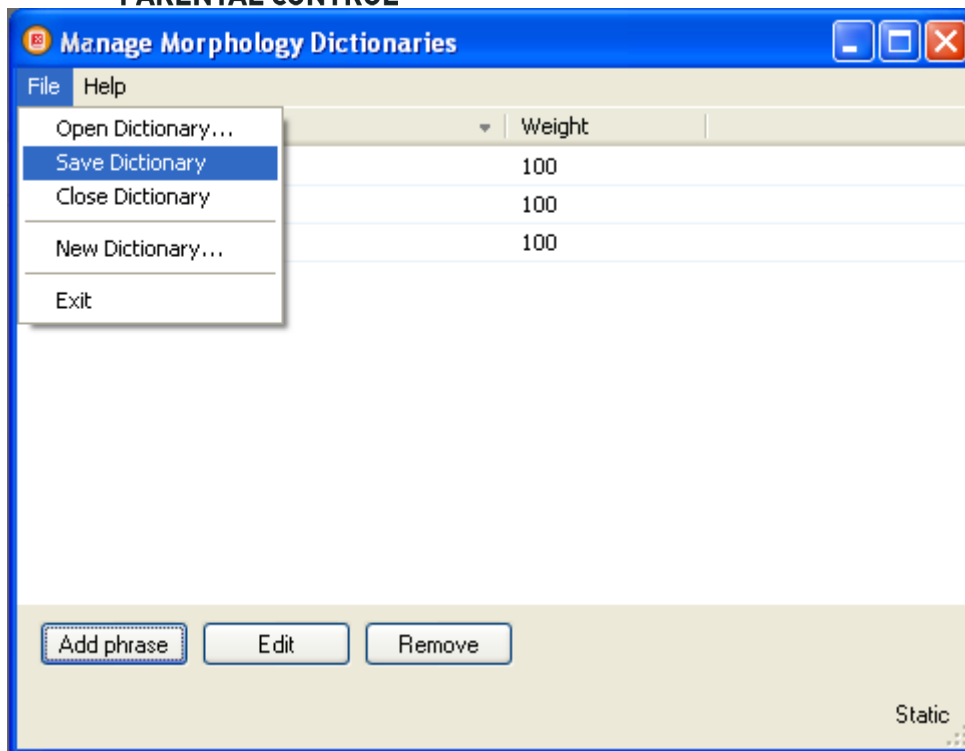
Opening a dictionary



Adding phrases



Adding a phrase and its weight

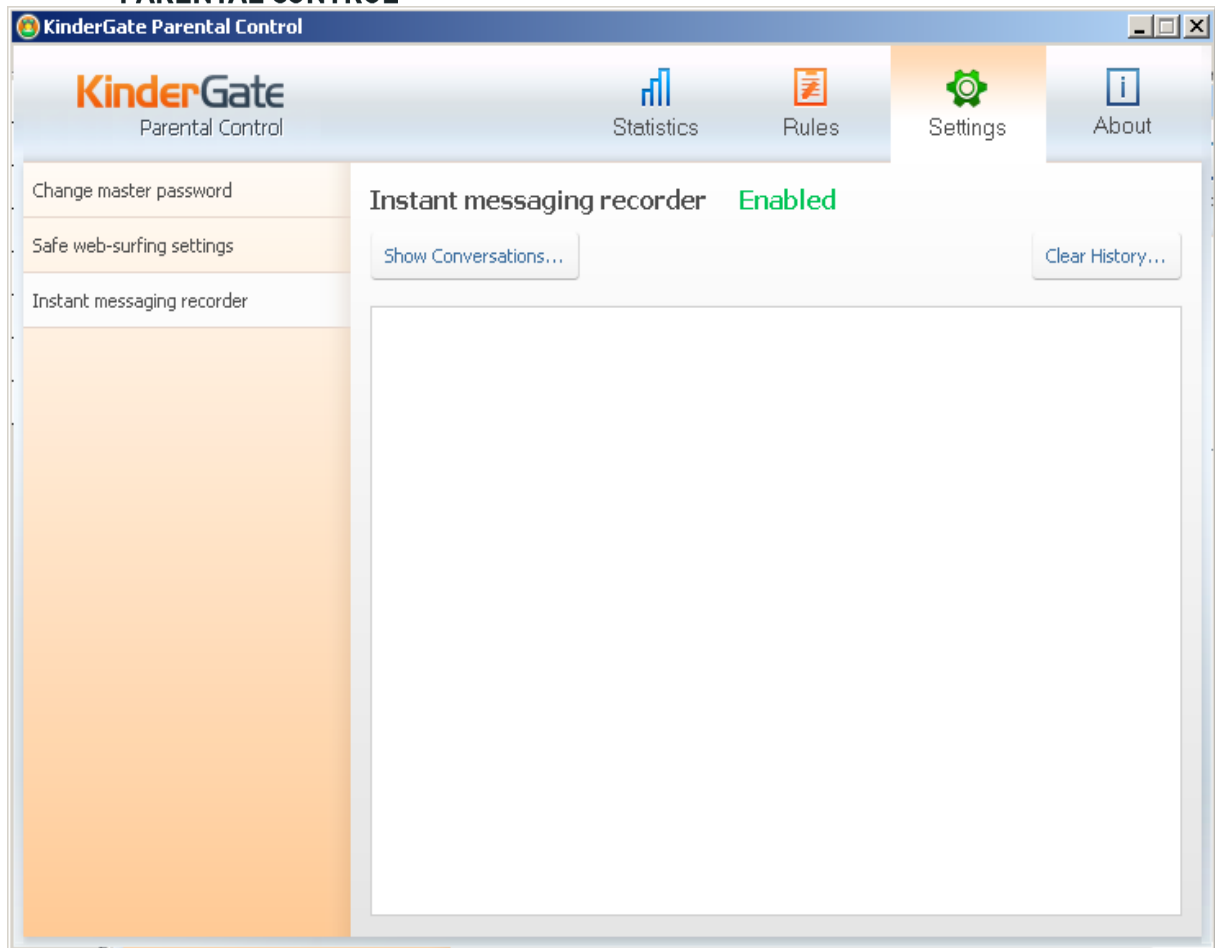


Saving the dictionary

## Instant Messages Recording

Version 1.2 can record messages that users exchange in instant messaging applications, such as ICQ, MSN and IRC, as well as in popular social networks, including vkontakte, odnoklassniki and facebook. The system only supports open data channels.

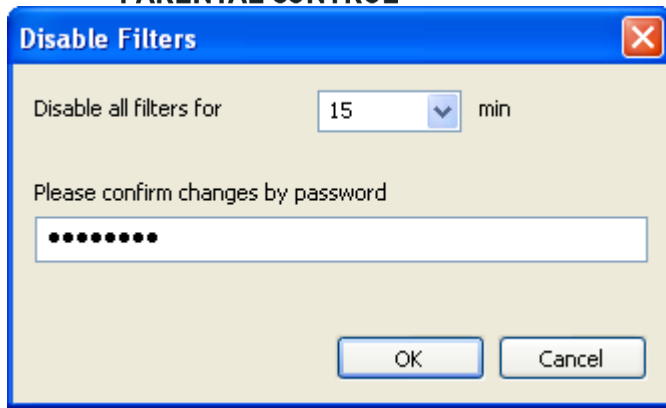
Use the switch on the “Instant messaging recorder” page to “Enable” or “Disable” this feature. You may the history of recorded conversations on the same page. Select two unique user IDs to show all messages exchanged by the users.



## Cancel Access Denial

If a user is trying to access a restricted resource, a KinderGate Parental Control message will appear in the browser window. You may allow access to such a resource by clicking the appropriate link in the browser window.

This will open a pop-up window where you will be prompted to enter KinderGate Parental Control administrator password and indicate the length of time to disable filtering.



**Caution!** With this mode on, KinderGate Parental Control disables all filtering features. The program will not cancel access restriction only for a specific resource.



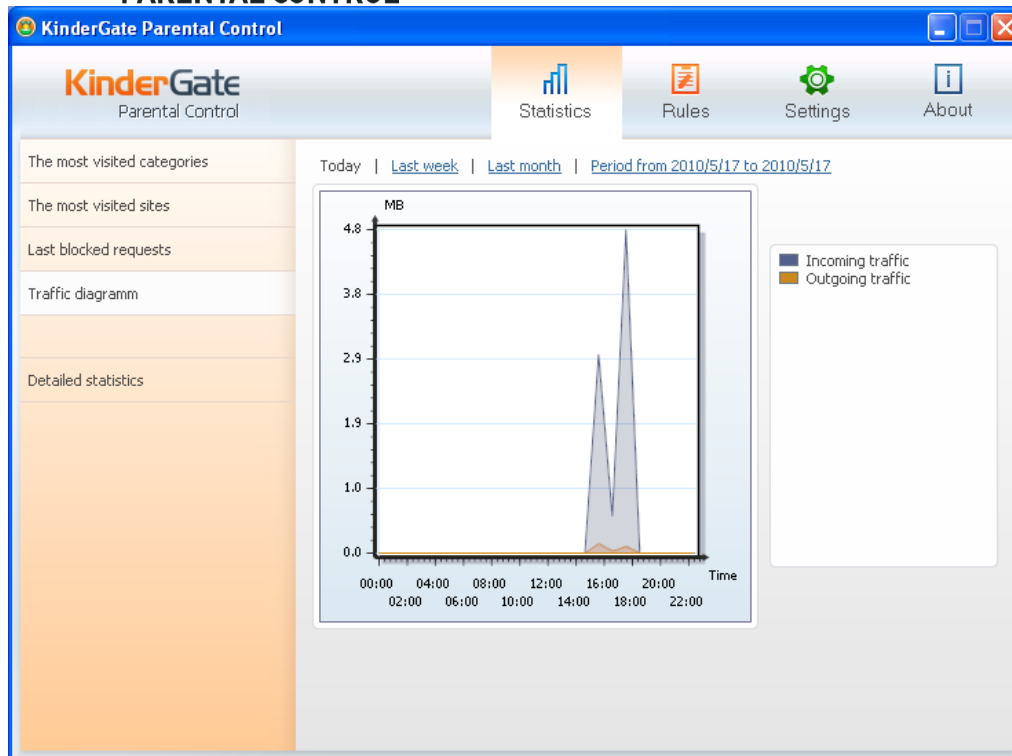
## KinderGate Parental Control Statistics

KinderGate Parental Control has an integrated statistics database where it records Internet access statistics, visited website addresses, incoming and outgoing traffic, website categories and access denial statistics. The statistics database is contained in an `ugpc.fdb` file located in `%KinderGate%` folder.

Statistics are shown in the KinderGate Parental Control Administrator Console on the Statistics page. Graphic representation is supported for the following statistics data:

- Most popular website categories
- Most popular websites
- Traffic graph





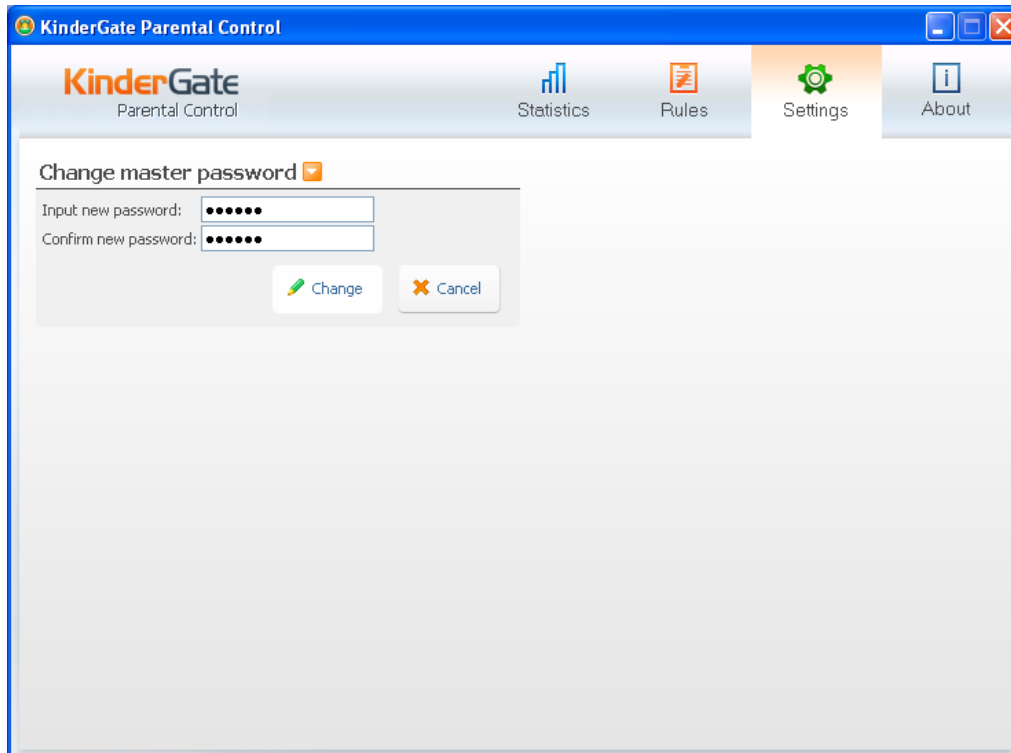
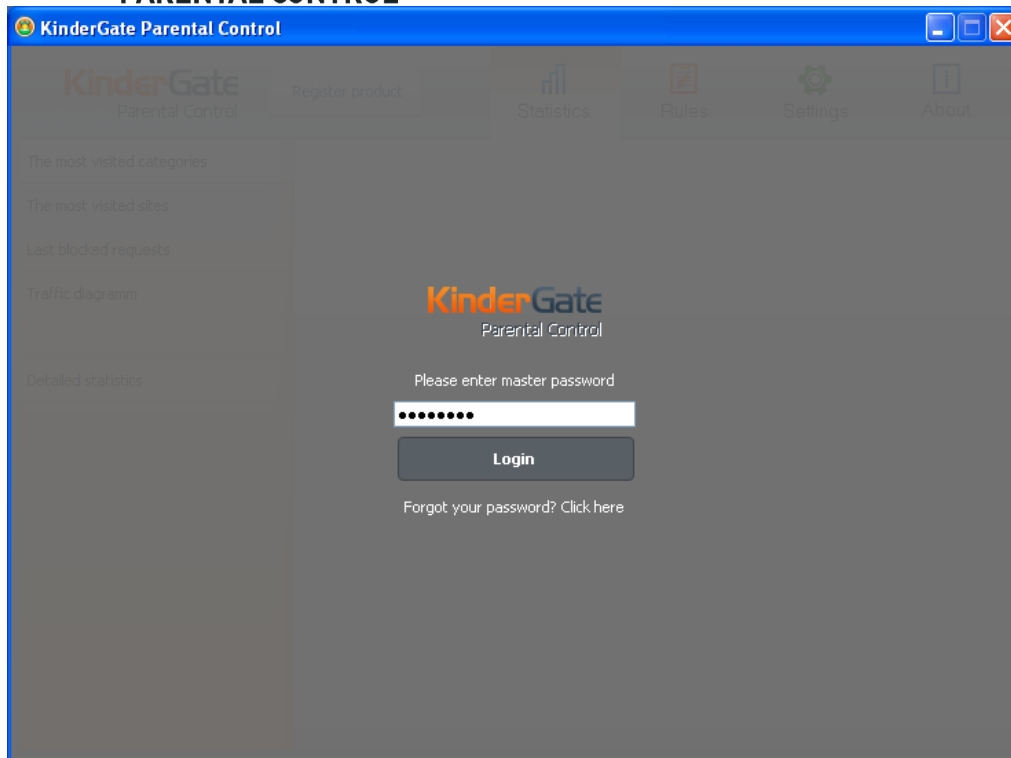
Access denial and detailed statistics are presented in charts.

## Password Recovery

The password assigned during installation will be required to establish connection between the Administrator Console and KinderGate Parental Control service. If for any reason you are unable to enter the correct password, type in a random password in the console. In this case, when you try to connect, the program will display a password recovery link. Click on the link.

# KinderGate

PARENTAL CONTROL



A new password will be sent to the Email address you specified during activation. Each new password is a randomly generated set of characters. You may change the new password on the “Settings” page of KinderGate Parental Control console.

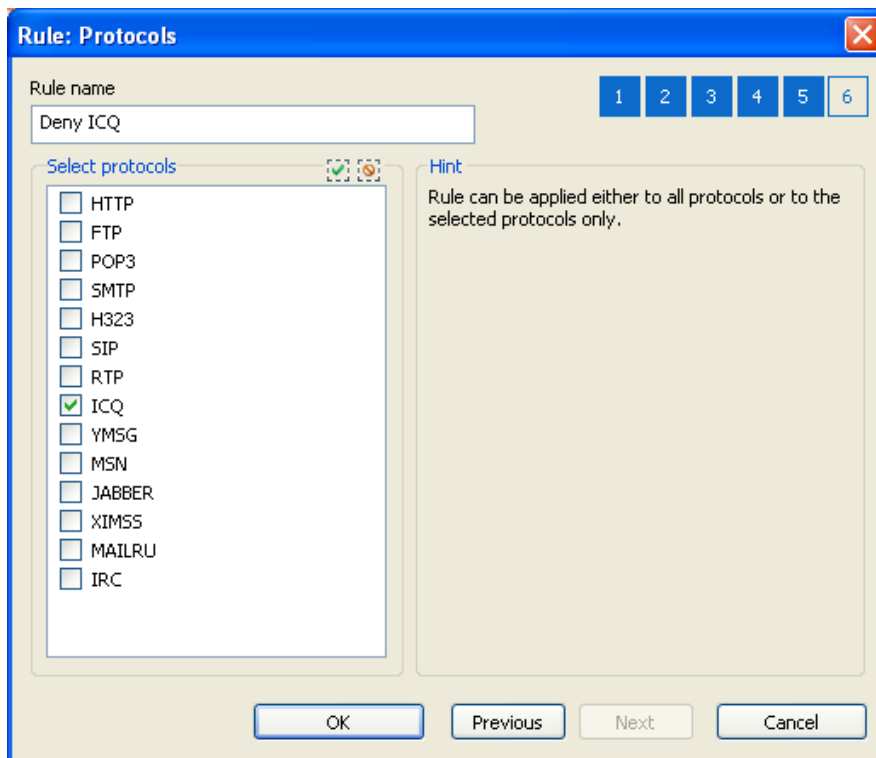
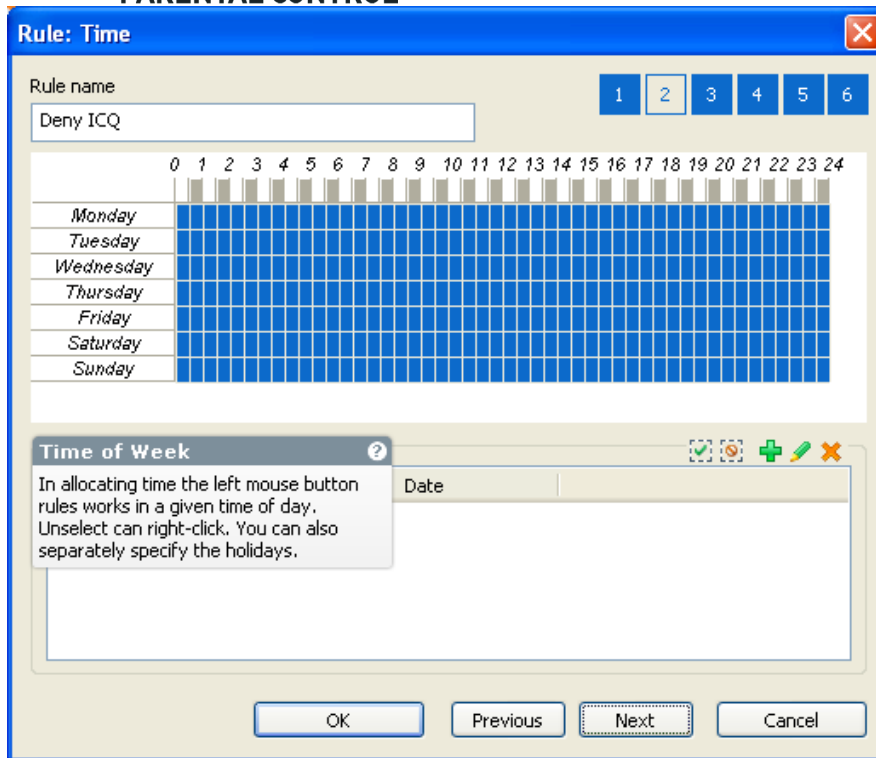
### Appendix

This Appendix contains examples of creating advanced filtering rules in KinderGate Parental Control. The examples cover some of the most popular restrictions.

#### ICQ client denial

The screenshot shows a window titled "Rule: General" with a close button in the top right corner. The window contains the following elements:

- Rule name:** A text input field containing "Deny ICQ".
- Logic type:** A dropdown menu set to "Match any condition".
- Hint:** A text area containing the text "Under the specified conditions the rule will close network connections."
- Buttons:** "OK", "Previous", "Next", and "Cancel" buttons are located at the bottom of the dialog.



You may use the same method to deny access over other protocols, including FTP, HTTP, POP3, SMTP, SIP, H.323, MRA (Mail-agent), MSN, Jabber, etc.

# KinderGate

PARENTAL CONTROL  
Social networks access denial

**Rule: General**

Rule name: Deny social network

Logic type: Match any condition

Hint: Under the specified conditions the rule will close network connections.

Rule Action Hint

OK Previous Next Cancel

**Rule: Site Categories**

Rule name: Deny social network

Input URL to check category: mspace.com

Check address

Select undesirable sites categories:

- Social Network
- Unknown
- Real Estate
- Computer and Internet Security
- Financial Services
- Business and Economy
- Computer and Internet Info
- Auctions
- Shopping
- Cult and Occult
- Travel
- Abused Drugs
- Adult and Pornography

Add categories Setup exclusions

OK Previous Next Cancel

## Hide pictures on a specific website

**Rule: General**

Rule name:

Logic type:

**Hint**  
Rule Action Hint

**Hint**  
Under the specified conditions the rule will close network connections.

OK Previous Next Cancel

**Rule: Addresses**

Rule name:

Input URL or IP to check blocking criteria:

Check address

**URLs list**

Address

Remove filters Setup exclusions

OK Previous Next Cancel

**Address** [X]

Enter address

(you can use '\*' to define group of sites, e.g. \*web-site.net\*)

[Add & Close] [OK] [Cancel]

**Rule: Content Types** [X]

Rule name:  [1] [2] [3] [4] [5] [6]

You can add a custom content type  
[Click here to find more content-types](#)

Select existing content-type or type new  
 [v]

Enter content-type

[Add type]

Select undesirable content-types

- application
- audio
- image**
  - gif
  - jpeg
  - png
  - tiff
  - vnd.microsoft.icon
- text
- video

[OK] [Back] [Next] [Cancel]

## Deny Web-mail category and allow access to [mail.yahoo.com](mailto:mail.yahoo.com) as an exception

**Rule: General**

Rule name:

Logic type:

Hint: Under the specified conditions the rule will close network connections.

Buttons: OK, Previous, Next, Cancel

**Rule: Site Categories**

Rule name:

Input URL to check category:

Check address

Select undesirable sites categories:

- Web based email
- Unknown
- Real Estate
- Computer and Internet Security
- Financial Services
- Business and Economy
- Computer and Internet Info
- Auctions
- Shopping
- Cult and Occult
- Travel
- Abused Drugs
- Adult and Pornography

Buttons: Add categories, Setup exclusions, OK, Previous, Next, Cancel

