# Table of Contents

Introduction .................................................................................................................. 3

About KinderGate ....................................................................................................... 4

KinderGate Features .................................................................................................. 5

Filtering Methods ...................................................................................................... 6

**KinderGate Installation** .......................................................................................... 7  
  System Requirements .............................................................................................. 7  
  KinderGate Installation on Computers with Microsoft Windows ......................... 7  
  Initial Settings and Registration ............................................................................. 7

**KinderGate License Registration** ......................................................................... 9  
  Trial License ............................................................................................................ 9  
  Commercial License ............................................................................................... 10

**KinderGate Updates** ............................................................................................ 13  
  Software Update for MS Windows .......................................................................... 13

**Uninstalling KinderGate** ....................................................................................... 14  
  Software Uninstall for MS Windows ...................................................................... 14

**KinderGate Filtering Settings** .............................................................................. 14  
  Starting the KinderGate Console .......................................................................... 14  
  Simple Administrator Console .............................................................................. 14  
  Advanced Administrator Console .......................................................................... 16  
    License .................................................................................................................. 17  
    General Settings .................................................................................................. 18  
    Morphology ......................................................................................................... 20  
    URL Categories .................................................................................................. 24  
    HTTPS filtering .................................................................................................... 26  
    Exclusions ............................................................................................................ 27  
    Requests ............................................................................................................... 29  
    Login History ...................................................................................................... 30  
    Statistics .............................................................................................................. 31

**Technical Support** ............................................................................................... 33

**Appendices** ......................................................................................................... 34  
  Appendix 1. Setting up a Local Certificate Authority Root Certificate .................. 34  
    Setting up the certificate for the Internet Explorer and Chrome browser in MS Windows .......................................................................................................................... 34  
    Setting up the certificate in Firefox browser .......................................................... 39
Introduction

The KinderGate Parental Control software (hereinafter – KinderGate) is used to control Internet access and protect minors from visiting dangerous and infected websites and resources associated with violence, extremism, drugs, pornography, suicide, unwanted dating sites, forums, etc.
About KinderGate

The KinderGate software solution filters websites by their content and prevents access to certain sites or Internet services, blocking or limiting access to websites with content not suitable for minors; it blocks advertisement, pop-up windows, banners, as well as access to social networks and videos.

KinderGate can be installed on school or home computers, providing reliable web surfing protection for Internet users.
KinderGate allows quick filter settings for any Internet connection by using a simple administrator console and more complicated filtering by using an advanced administrator console; it also enables to review web-surfing statistics and to monitor website connection status.

Website classification and blocking is done by analyzing text for a certain set of words in UserGate built-in dictionaries, such as “Bad Words”, “Drugs”, “Gambling”, “Pornography”, “Suicide”, or “Terrorism”.

The users have an option to create their own dictionaries and to populate them with key words; to set up Internet settings parameters, specifying website categories to be blocked; to manage website access of any user allowing or blocking access to various Internet resources.

The software solution is an effective and precise Internet filter that does not restrict access to harmless resources.
Filtering Methods

The KinderGate software solution combines URL-filtering capabilities with filtering by website category; it has a large set of mechanisms for checking traffic and can block access to an entire site or to its parts using the following methods of HTTP filtering:

- By website category (UserGate URL Filtering 4.0);
- Morphological analysis and regular expressions;
- Control of downloaded files by type;
- Safe Search function;
- Contextual advertising filtering;
- Black and white lists.
KinderGate Installation

System Requirements
KinderGate software can be installed on computers with Microsoft Windows 7/8/10, connected to the Internet. KinderGate requires at least 2 GB RAM and 200 MB free space on the hard drive to work efficiently.

KinderGate Installation on Computers with Microsoft Windows
KinderGate software is installed by launching an installation file, which opens the Installation Wizard dialog window.

Installation Wizard automatically performs all procedures required to install KinderGate: decompresses files, creates additional KinderGate system service, as well as installs the necessary drivers.

KinderGate is installed in the %Program Files%\UserGate\KinderGate folder by default (hereafter – simply %KinderGate%).

Please restart your computer after installation.

Initial Settings and Registration
After installation is complete, you must set up the initial filter settings and register the product.

To begin initial software setup start the KinderGate management web console. You can do it in either one of the following ways:

1. Open a web browser and go to http://localhost:8001.
2. Start the KinderGate management console from the application list.

When you first start the console you will be requested:

1. To select the interface language, for example English, and click the Continue button:

   ![Image of Installation Wizard with language selection options]

   2. To read the License Agreement; to click the Accept button to continue installing the KinderGate software:
3. Set the KinderGate administrator password;
KinderGate License Registration

To register the KinderGate license you will need to use the administrator console, a special PIN code, and an Internet connection.

When you first start the administrator console, the Product Activation Wizard is automatically launched. The Product Activation Wizard allows receiving a trial or a full-feature KinderGate key. The key must be requested online, by sending an HTTPS request to the manufacturer’s website (http://www.usergate.com/). In order to register the license correctly, HTTPS protocol must be enabled.

**Trial License**

When requesting a trial key, a trial license, active for 30 days is generated. When the trial version of the license expires, KinderGate software no longer works and Internet access is blocked.

To receive the trial key, in the Registration Activation Wizard dialog window:

- Check the Get Trial License box;
- Click the Next button:

- Enter registration name, personal information, E-mail, country, and region or state to continue program installation:
Commercial License
To register a commercial license, in the Registration Activation Wizard dialog window:

- Select Enter PIN Code;
- Enter the special PIN code received when purchasing the KinderGate software in the text field;
- Click the Next button:
Enter registration name, personal information, complete the required fields to continue program installation, and enter E-mail for follow-up;
Click the Next button:
If you ever lose your KinderGate password, an e-mail with a new password will be sent to the address entered during software activation.
KinderGate Updates

UserGate continuously works on improving the KinderGate software. You will learn about a new version release by receiving a new message in the web console License section.

Software Update for MS Windows

Download the new version of KinderGate from the manufacturer’s website and install it without deleting the current version. Once the installation is complete, restart your computer.
Uninstalling KinderGate

**Software Uninstall for MS Windows**

Uninstall the software using the standard MS Windows program management tools (Control Panel--Programs and Features).

**KinderGate Filtering Settings**

**Starting the KinderGate Console**

You can start the KinderGate console in one of two ways:

2. You can start the KinderGate control console from the applications list.

When you start the KinderGate software, an Authentication window opens where you need to enter the administrator password and click the Login button:

![Authentication Window](image)

The KinderGate software has a Simple or an Advanced administrator console for setting filters. A simple administrator console opens when you start KinderGate.

You can change the administrator console by clicking on Switch to Advanced Console in the KinderGate page header:

**Simple Administrator Console**

The simple administrator console is used to review filter settings, quickly enable/disable filters, change filter level, check URLs, add sites to black or white lists, update the basic use report, enable/disable additional checking, or switch to the advanced administrator console.

The header of the Simple administrator console on the KinderGate page has information on the installed version of KinderGate, the owner of the registered license, and the license expiration date.

The Simple administrator console page has the following functional sections:

- Filters (Enable/Disable);
- Filtering (select filtering level – minimal, medium, high, maximum, allow everything, custom categories);
- Site check;
- Statistics;
The Filtering section is used to select the level of filtering and website blocking by selected categories. The filter level automatically blocks access to a pre-determined set of website categories. You can select the filter level from a drop-down menu which has the following items:

- Allow everything;
- Minimal;
- Medium;
- High;
- Maximum;
- Custom Categories.

The Allow Everything filter level will remove filtering by pre-determined set of categories and the categories will not be blocked. A certain list of blocked website categories corresponds to each level of filtering. For example, when you choose the Minimal level of filtering the following categories will be blocked:

1. Advertising and pop-ups;
2. Phishing and fraud;
3. Malware;
4. Pornography and violence;
5. Nudity;

The Custom Categories level lets the user select and block categories.

You can select categories in the drop-down menu in URL Categories list which appears when you click Select. Once you select the categories click the Apply button.

The Site Check section is used for quickly checking website. In order to do that, in the Enter the URL Address to View or Set Classification text field, enter the website address and click the Check button. Information on website category will appear:

The Content downloading section is used to set permissions for downloading video, audio, images, documents, archives and executables, or FLASH by pointing the mouse and clicking on the word Enabled/Disabled.

The Statistics section provides statistics on Internet usage by the number of network requests and responses to them.

The Change Password section enables changing the old administrator password to the new one. In order to do so, enter the old and new passwords and confirm the new password in the text fields with the appropriate names, then click the Change button.

Advanced Administrator Console

The advanced administrator console can be used to fine-tune secure Internet access or for blocking advertising and banners.

The advanced administrator console has the following sections:

- Parental Control:
- License;
- General settings;
- Morphology;
- URL categories;
- Exclusions;
- HTTPS filtering;
- Requests;
- Login history.
- Statistics;
- Enable/Disable Filters button.
The Enable/Disable button is used to quickly enable/disable all filters and is located in the functional section at the bottom of the expanded Administrator console.

License

The License section is used to register the license or review information about the type of the installed KinderGate version and its expiration date.

A New Version is Available link appears if there is a new version at the manufacturer's website. Follow the link to go to the new version page and to download the updates.

The License section has the following information:

- Version;
- Type of version: trial, registered, unregistered;
- License expiration date;
- Registration name;
- Module name and registration expiration date;
- Information on the nodes of a cluster license.
The License page has the following functional features:

- **Registration** – to register the license;
- **Support** – a link to the technical support website;
- **Help** – a link to the online guide;

**General Settings**

The General Settings section is used to set up interface language, time zone, safe search, ad block; to disable/enable content download, create certificates, or change administrator password.

The General Settings page has the following sections:

- Admin console settings;
- Search;
- Ad block;
- Content downloading;
- SSL Certification Authority;
- Change password.

The **Admin Console Settings section** is used to set up interface language and time zone. Time zone is responsible for correctly displaying statistics, event log, and login history (in the applicable time zone). The default interface language and time zone can be selected from the drop-down menus. The drop-down menu can be opened by pointing the mouse and clicking on the selected interface language, for example English, and time zone, for example Australia/Brisbane:
The Search section is used to enable/disable the safe search option on search engine websites such as Google, Yandex, Yahoo, Bing, Rambler, as well as YouTube and others. Once safe search is turned on, a mechanism is enabled that does not allow unauthorized content, pornography or bad words, for example, to be found using the search engine. Not only websites are filtered, but also pictures and videos.

You can enable/disable safe search by pointing the mouse and clicking on the word Enabled/Disabled:

The Ad Block section is used to block advertisements, pop-ups in downloaded websites, to view information on the current version or the latest updates.

The problem of pop-ups is becoming more and more prevalent. Oftentimes, following a link hidden behind an annoyingly persistent picture has nothing to do with a user’s conscious decision, but is simply a wrong mouse click. KinderGate software blocks pop-ups, including those downloaded from other websites.

Pervasive banners will not leave you alone when you surf the web. Visiting a harmless site might well involve watching pornographic images located, for example, on the side of the page. KinderGate software solves this problem as well, acting as a "banner chopper".

You can enable/disable Ad Block by pointing the mouse and clicking on the word Enabled/Disabled:

The Content downloading section is used to set permissions for downloading video, audio, images, documents, archives and executables, or FLASH by pointing the mouse and clicking on the word Enabled/Disabled:
SSL Certification Authority section allows setting up a certificate used for SSL protocol encryption on the local computer, which will help avoid browser notifications of SSL certificate security issues in filtering sites that use the HTTPS protocol.

The certificate must be set up for the HTTPS traffic to be filtered correctly.

To receive the certificate click on the Download CA Certificate in the SSL Certification Authority dialog window.

The certificate needs to be setup in all browsers used on the computer. Information on certificate setting in various browsers can be found in Appendix No. 1 to this Guide.

The Change Password section enables changing the old administrator password to the new one. In order to do so, enter the old and new passwords and confirm the new password in the text fields with the appropriate names, then click the Change button:

Morphology

The Morphology section is used to analyze web pages for certain words and word combinations and contains pre-set morphology dictionaries.

Morphological analysis allows recognizing certain words or word combinations on a web page, as well as blocking access to the entire web page if it contains unauthorized words, and controlling access to certain website sections without blocking the entire resource at the category or domain level.

This method is effective if the others cannot block access to resources or groups of resources that are similar in content. Morphological analysis works for controlling access to social networks, forums, and other websites whose content depends mostly on the users.

KinderGate reviews the text on a page and calculates its total “weight” based on the “weights” of words and word combinations in the morphological categories of the application dictionaries. If the “weight” of the page exceeds the “weight” of the morphological category, KinderGate returns a message that the access is blocked.

In calculating the “weight” of a page, all forms of unauthorized words are used. In searching for word forms KinderGate uses built-in Russian, English, German, Japanese, and Arabic dictionaries.

KinderGate software has the following morphology dictionaries provided by UserGate that are Enabled by default:
• Bad Words;
• Drugs;
• Gambling;
• Pornography;
• Suicide;
• Terrorism.

Built-in morphology dictionaries cannot be edited or deleted, however, the dictionaries can be Enabled/Disabled or the filtering level can be changed in setting the HTTP filter rules on the Morphological Settings page.

Morphological filtering is set up in the Morphology section on the Morphological Settings page:

Morphology dictionaries provided by UserGate are constantly updated.

You can see the information on the latest update of the list of words in a dictionary and the version number by pointing the mouse over the dictionary icon.

To disable a morphology dictionary simply uncheck the box next to it. In addition, you can change the threshold for each of the dictionaries provided. There are three filtering levels: low, medium, and high. You can select the filtering level for each morphology dictionary by pointing the mouse and clicking on the level.

Creating a Morphological Database

The users can create their own morphology dictionaries. A morphology dictionary can be created in the Morphology Dictionaries and Selected List sections on the Morphological Settings page.
To create a morphology dictionary, click on the Add button in the Morphology Dictionaries section. In the Dictionary Properties dialog window:

- Enter dictionary name;
- Set the dictionary status and threshold;
- Enter the source address (for auto updates);
- Click the OK button:

In the Selected List section you can add words to the created dictionary by which the content of the web pages will be filtered.

To add a word to the list you need to:

- Click the Add button;
- Enter the word into the text field;
- Enter the word “weight” (equals 100 by default):

In adding a word to the morphology dictionary you can use the “!” modifier in front of the word, “!bassterd”, for example. In that case a slang word will not be transformed into various word forms, which will reduce the probability of false blocking. You can enter both words and word combinations in the category list.

If necessary, words in a dictionary can be edited or deleted, do to that highlight the word and click on Edit or Delete. Edit the word directly on the word line; delete the word by clicking Delete.

To delete all words in a dictionary use the Clear button. You can delete a list of words by clicking Delete.

**Creating a Centrally Controlled Morphological Database**

The Administrator may create personal dictionaries and distribute them on all computers that have KinderGate. Follow these instructions to create a morphological database:
1. Create a list.txt file with a list of words in the following format:

```
!word1 !word2
!word3
word4 50
...
lastword lastweight
```

**Note:** The dictionary weight is equal to 100 by default, but may be changed.

2. Create an archive of the file named list.zip;

3. Create a version.txt file and indicate the database version number within the file, 2, for example. You must increment this value with each update of the morphological database;

4. Post the created zip file and version.txt file on your website so that they are available for download;

5. Create a morphological database on each computer where KinderGate is installed;

6. Enter the address for update downloads. KinderGate will check for a new version of the dictionary on your website twice a day and update it as necessary.

### Deleting a Morphology Dictionary

You can delete a morphology dictionary by clicking the Delete button in the Morphology Dictionaries section and then Delete in the dialog window:
URL Categories

The URL Categories section is used to select the level of filtering and blocking by given categories, to check websites, or to change filtering categories and to request a category change for the selected website.

Filtering level automatically prevents access to pre-set site categories. You can select filtering levels from a drop-down menu that has the following items:

- Allow everything;
- Minimal;
- Medium;
- High;
- Maximum;
- Custom categories:

The Allow Everything filtering level disables filtering by pre-set categories and, consequently, the categories will not be blocked.

Each filtering level has a certain list of blocked site categories associated with it. For example, when Minimal level is selected, the following categories will be blocked:

- Advertising and popups;
- Phishing and fraud;
- Malware;
- Pornography and violence;
- Nudity;
- Botnets:
The Custom Categories level lets the user select and block all necessary categories. Category selection is done in the drop-down menu in URL Categories, which appears when you click Select. Once you select the categories click the Apply button:

The text field Enter URL Address to View or Set Classification is used to check the site category, to request a category change if the current category does not match the site content, and to check which morphological database is blocking the address entered (when using a morphological filter).

When Entering URL Address to View or Set Classification in the text field, please:

- Enter the URL address;
- Click the Check button.

If the site has already been entered into any controlled site category, the Gambling category on the Secure Connection page, for example, after you click the Check button, you will see the name of that category:
If you believe that the site category does not match its content, you can send a request to UserGate to change the category as follows:

- Select the category from the Suggest Category for Current URL drop-down menu;
- Click the Suggest URL button:

Once you send the category change request, you will see a message: “Your category change request for this site has been accepted”.

**HTTPS filtering**

The TTPS filtering section is used to setup HTTPS content filtering. To monitor HTTPS the Man-In-The-Middle technology that allows content decryption is used. Decryption is done for websites or website categories specified on this page. After decryption, filtering is done according to set rules (morphology, black and white lists, site categories, etc.).

- **The Inspected URL Categories section** allows setting website categories for which HTTPS content decryption will be done;
- **The Inspected Domains section** allows setting a list of websites for which HTTPS content decryption will be done. You can use wildcard “*” when entering websites – *.facebook.com, for example:
Important! While using HTTPS filtering a user may receive a message that there is a problem with the server certificate. To avoid such messages, please download and set up the authentication certificate on your computer. Please see Appendix No. 1 to this Guide for more details.

Follow these steps for HTTPS filtering:
- Select categories or URLs for websites to be filtered. To filter all websites enter “*” in URL list;
- Download and set up the SSL certificate in the General Settings section.

Exclusions
The Exclusions section is used to create and keep the black and white lists of websites.

The Exclusions section contains pre-set standard black and white website lists that are automatically updated by UserGate.

Black website lists are lists that contain websites that will always be blocked. White website lists are lists that contain websites access to which will always be allowed. If the same Internet resource (URL) exits in both a black and a white list, the black list will have priority, i.e. the Internet resource will be blocked.
You can use wildcards in the lists:

- * – Any number of any symbols;

List formats are shown in the table:

<table>
<thead>
<tr>
<th>Example of Record</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>yahoo.com</td>
<td>The entire domain and all URLs of this domain are blocked, 3rd-level domains are not blocked</td>
</tr>
<tr>
<td>yahoo.com*</td>
<td>The entire domain and all URLs of this domain are blocked, 3rd-level domains are not blocked</td>
</tr>
<tr>
<td><em>.yahoo.com</em></td>
<td><a href="http://any.yahoo.com/any/">http://any.yahoo.com/any/</a> is blocked</td>
</tr>
<tr>
<td>yahoo.com/12345/qwer</td>
<td>yahoo.com/12345/qwer only is blocked</td>
</tr>
<tr>
<td>yahoo.com/12345/*</td>
<td>yahoo.com/12345/ any/</td>
</tr>
</tbody>
</table>

Users can create their own black and white lists. In addition, in large corporations the Administrator has an option of creating lists and centrally distributing them on all computers where KinderGate is installed. Follow these instructions to create a list:

1. Create a text file list.txt with a list of URLs in the following format:

   www.site1.com/url1
   www.site2.com/url2
   ...

2. Create an archive of the file named list.zip;

3. Create a version.txt file and indicate the database version number within the file, 2, for example. You must increment this value with each update of the list contents;

4. Post the created zip file and version.txt file on your website, so that they are available for download; for example, at the following addresses:
   http://companyweb.com/filtering/list1/list.zip;

5. On each KinderGate computer create an updatable list and enter the address for update downloads. KinderGate will check your website for a new version twice a day and update it as necessary.

You can see the information on the latest list update and version number by putting the mouse over the website icon in the list.

Requests

The Requests section is used to add harmless sites to white lists and to display information on user requests to add blocked websites to the white list.

User requests are displayed on the Requests page and enable Administrator to:

- Go to the website to view its content;
- Add the user-requested URL to the white list if the site is harmless;
- Delete the white list request if the requested site is unauthorized or dangerous;
- Update the information displayed on the page;
- Determine the node (computer) from which the request was sent:

When an attempt is made to access a blocked URL the user sees a KinderGate Blocked message used to display information about the blocked site (URL, category, reason), to send a white list request, or to unblock the site.
When the user receives a Blocked message he or she may send a request to unblock the site to the Administrator by clicking on Ask Administrator to Add This Site to White List.

The blocked URL will be displayed on the Requests page of the Administrator console. The user request to unblock the site needs to be analyzed by the Administrator. If the website is harmless, the Administrator may decide to add the site to a white list by clicking the Add to White List button:

The URL of the requested site will be moved from the Requests to the Exclusions section, White List under the Exclusion List.

**Login History**

Login history is used to display history of setting changes and actions of system administrator, authentications on a specific computer node or a group of computers tied into a cluster.

The Login History page has information on the date of login, user name, user node, initial IP address, and has the following functional features:
• Export – to export login history to a local drive as a text file;
• Clear the entire list:

The Login History page has the navigation line at the bottom of the page. The navigation line is used to navigate the pages and to refresh the login history:

Statistics
The Statistics page is used to collect, view, and update statistics on Internet use by the number of network requests and responses to network requests.

Information on the number and type of outgoing network requests has the following status:

• Blocked;
• Allowed;
• Ad block requests.

Information on the number and type of network responses has the following status:

• Blocked;
• Allowed.
Technical Support

The Technical Support section can be found at https://support.usergate.com/ where there is additional information on setting up KinderGate. In addition, you can send a request for help on a problem or find an answer to a question in the company Knowledge Base.
Appendices

Appendix 1. Setting up a Local Certificate Authority Root Certificate

Setting up the certificate for the Internet Explorer and Chrome browser in MS Windows

Open the folder into which you downloaded the certificate and double click on it (user.der):

Certificate Information window will open. Click on the Install Certificate Button:
Certificate Import Wizard will launch. Complete the import following all recommendations of the Certificate Import Wizard:
Select Place certificate in the following store and click Browse:
Select Trusted Root Certification Authorities and click OK:

Then click Next and then Finish:
When security warning appears click Yes:

You are about to install a certificate from a certification authority (CA) claiming to represent:

kindercontrol.com

Windows cannot validate that the certificate is actually from "kindercontrol.com". You should confirm its origin by contacting "kindercontrol.com". The following number will assist you in this process:

Thumbprint (sha1): CFFC8EC6 060A60E1 AC40D535 D2559460 17FDF20E

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?
Certificate setup is complete.

**Setting up the certificate in Firefox browser**

Setting up the certificate in Firefox browser is similar for all operating systems. Let's review the setup using MS Windows.

Open Firefox Settings (Tools--Options):

Go to **Advanced** and select the **Certificate** tab. Click on the **View Certificates** button:
Click the Import button and specify the path to the downloaded certificate (user.der file):
Checkmark **Trust this CA to identify websites** and click OK:
Certificate setup is complete.