Kerio Administration Console

Help

Kerio Technologies

Printing Date: February 5, 2008

This brief guidelines refer to *Kerio Administration Console* in version *2.3.3*. All additional modifications and updates reserved.

Contents

Chapter 1

What is Kerio Administration Console?

The *Kerio Administration Console* application (from now on labeled as *Administration Console*) is used for administration of *Kerio Technologies'* server products (*Kerio WinRoute Firewall* and *Kerio MailServer*).

Kerio Administration Console is an independent application which communicates with a server application (service) via a special network protocol. This enables use of *Administration Console* for local administration (from the computer where the service is running), as well as for remote administration (from any workstation in the Internet). All network communication between *Administration Console* and the server application is encrypted so that transmitted data is protected from tapping and misuse.

Administration Console enables single connections to the server (login data are not saved) as well as creating of so called bookmarks (login information is saved and used for following connections by certain servers).

Administration Console is conceived as a modular application. It is based on a simple program (referred as *the main window*) which enables basic configuration (e.g. setting of a language for the administration interface) and specification of login data. Depending on a version and type of the server application, a corresponding administration module is started where the server application can be configured and its status can be monitored. Thanks to this modularity, *Administration Console* provides compact environment for administration of various versions of server applications at various servers.

Chapter 2

Installation, File Location and Startup

This chapter provides detailed information about installation, file location and startup of the *Administration Console* on — *Windows*, *Linux* and *Mac OS*. Information on system requirements and supported versions of individual operating systems are listed in guides referring to particular server applications.

Notes:

1. *Kerio WinRoute Firewall* is designed for *Windows* only. The corresponding administration module is also available for this operating system only.

2. It is not necessary know location of files for basic maintenance *Administration Console*. However, knowledge of file location is needed for adding of new help files (only on *Windows* — see chapter 3.7), new localizations (refer to chapter 3.6) and exporting created bookmarks to another computer.

2.1 Windows Operating Systems

Administration Console is installed along with the *Kerio WinRoute Firewall* and/or the *Kerio MailServer* (represented by the *Administration Console* component in the custom installation). At the server, it is not necessary to use the installation package to install *Administration Console*.

Administration Console can be started form the *Start* → *Programs*→ *Kerio* → *Kerio Administration Console* menu from the *WinRoute Engine Monitor* or *Kerio MailServer Monitor* context menu (for details, see guides referring to corresponding products).

Files location

The *Administration Console* installation file is stored in the `Admin` subdirectory of the directory where *Kerio Technologies* products are installed (typically `C:\Program Files\Kerio\Admin`).

The *Administration Console's* executable file (`kadmin.exe`) as well as individual administration modules (`wradmin*.exe` and `mailadmin*.exe`) and relevant dynamic libraries (`*.dll`) are stored in the directory.

The `translations` subdirectory includes localization files (`*.qm`) and the `help` subdirectory contains help files in the *HTML Help* format (`*.chm`).

Bookmarks (login data for individual servers) are saved in corresponding user profiles (each user has an own set of bookmarks). Each bookmark is saved in a separate file in the `C:\Documents and Settings\user\Application Data\Kerio\Admin` directory (in case of the *Windows 2000/XP/2003* operating systems), or

`C:\Users\user\Application Data\Kerio\Admin`

(in case of the *Windows Vista* operating system), respectively.

`C:\Documents and Settings\uzivatel\Application Data\Kerio\Admin`.

File suffix depends on application for which it is created (`.bkwf` for *Kerio WinRoute Firewall* and `.bkms` for *Kerio MailServer*).

Installation of the Administration Console for remote administration

For remote administration of a server application, only the *Administration Console* needs to be installed on the workstation. For this purpose, use the installation package of *Administration Console* for the corresponding product (the file name starts with `kerio-kwf-admin` or with `kerio-kms-admin`).

To run the installation, simply start a corresponding installation package. If an older version of *Administration Console* or *Administration Console* for another product is already installed at the workstation, it is not recommended to change the default installation directory!

If the *Administration Console* has been installed successfully, you can run it through *Start* → *Programs*→ *Kerio* → *Kerio Administration Console*.

2.2 Linux Operating System

The version for *Linux* is distributed only in a separate RPM package (its name starts with `kerio-mailserver-admin`). It is necessary to install this package both at the server (for local administration) and on hosts from which remote administration will be performed.

To install *Administration Console*, use this command:

`rpm -i <installation_package_name>`

e.g. `rpm -i kerio-mailserver-6.1.2build573-linux.i386.rpm`

If *Administration Console* is already installed, you can upgrade to the newer version using the following command:

`rpm -U <installation_package_name>`

To uninstall *Administration Console*, use this command:

```
rpm -e kerio-mailserver-admin
```

Starting Administration Console

Administration Console is started by the `kerioadmin` script. The script is stored in the `/usr/bin` directory. By default, the path is set so that it leads to this directory.

Warning: Administration Console should always be started by this script. If the `kadmin` file is started directly, it might happen that an incorrect version of the *Qt* library is downloaded (or that the library is not found) which would lead to incorrect functionality of *Administration Console*.

Files location

Administration Console is installed to the `/opt/kerio/admin` directory. The *Administration Console's* executable file (`kadmin.exe`) as well as individual administration modules (`mailadmin*.exe`) and relevant dynamic libraries (`lib*`) are stored in the directory.

Localization files (`*.qm`) are stored in the `translations` subdirectory. Help is not available in *Linux*.

Bookmarks (login data for individual servers) are saved in the `.kerio/admin` subdirectory of the home directory of the current user (there is a special set of bookmarks customized for each user). Each bookmark is saved in a separate file. The file extensions correspond with the application for which the bookmark refers (currently, the only alternative available is `.bkms` for *Kerio MailServer*).

2.3 Mac OS

Administration Console is installed along with *Kerio MailServer*. At the server, it is not necessary to use the installation package to install *Administration Console*.

Administration Console can be started from the *System Preferences* → *Other* → *KMS Monitor* → *Administration Console*.

Files location

Administration Console is installed to the `/Applications/Kerio MailServer` directory. Thid directory includes the `Administration Console.app` package. The `Contents/MacOS` subdirectory contains the main executable file, `Administration Console`, whereas the `Contents/Resources` subdirectory includes individual modules (`mailadmin*`).

Localization files (`*.qm`) are stored in the `Contents/Resources/translations` subdirectory. Help is not available on *Mac OS*. However, the `/Applications/Kerio MailServer` directory includes *Kerio MailServer* user's guide in *PDF*.

Bookmarks (login data for individual servers) are saved in the `.kerio/admin` subdirectory of the home directory of the current user (there is a special set of bookmarks customized for each user). Each bookmark is saved in a separate file. The file extensions correspond with the application for which the bookmark refers (currently, the only alternative available is `.bkms` for *Kerio MailServer*).

Installation of the Administration Console for remote administration

For remote administration of *Kerio MailServer*, only the *Administration Console* needs to be installed on the workstation. The installation is realized by a separate installation package (disk image) of *Administration Console* (its name starts with `kerio-mailserver-admin`).

To install *Administration Console*, use the wizard which is started when the image of the particular disk is opened. *Administration Console* can be started from the *System Preferences* → *Other* → *KMS Monitor* → *Administration Console*.

Chapter 3

Program Control

3.1 Main Dialog Window

Upon the *Administration Console* startup, the main dialog window will be displayed that includes all created bookmarks and the *New Connection* icon for single connection to the server or for creating of a new bookmark.

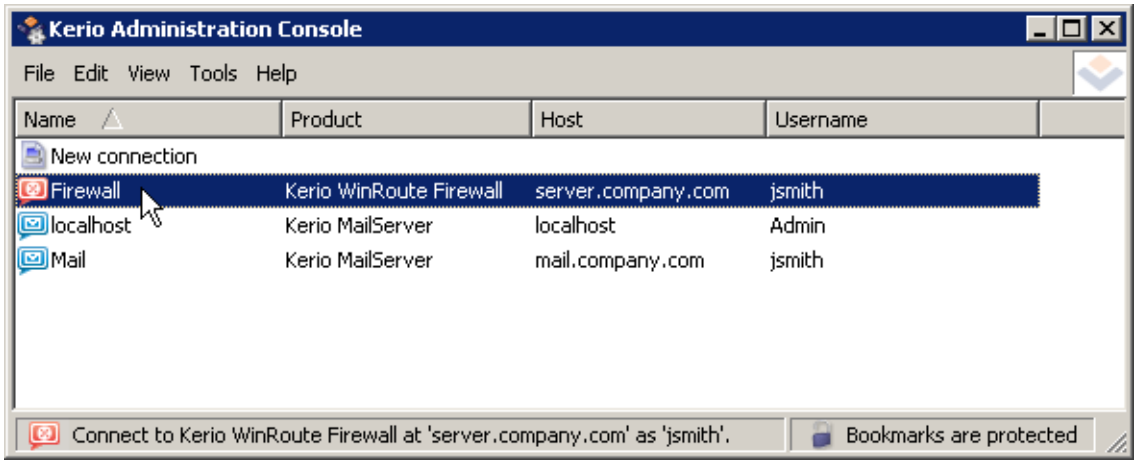

Figure 3.1 Administration Console's main window

Placing the mouse pointer over a bookmark displays detailed information on the corresponding bookmark at the bottom of the dialog window (name of a server application, server name or IP address, username). Double-click on a bookmark (or hold the *Enter* key or use the *File / Connect* option in the main menu) to connect to a corresponding server. If the password is not saved in a bookmark (see chapter 3.2), it will be required upon a connection attempt.

3.2 Connection to the server and how to create bookmarks

Double-click on the *New Connection* icon or select *File / New Connection* in the main menu to open the *New Connection* dialog window.

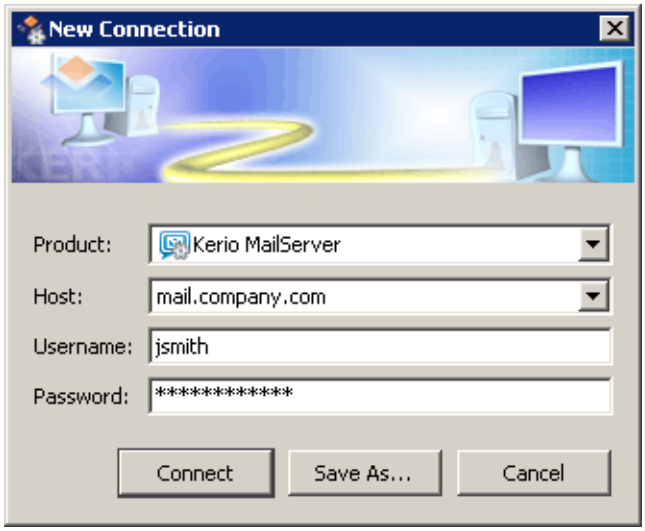

Figure 3.2 Setting connection to a server application

Product

Selection of a server application which will be administered.

Upon the startup, the *Administration Console* detects available administration modules and sets corresponding items for this entry. If administration program is not available for a particular application, connection cannot be established and a bookmark cannot be created.

Server

DNS name or IP address of the computer on which the server application is installed.

If you intend to connect to the server application from the computer where it is installed, specify server name as `localhost` (i.e. loopback).

We recommend not to use IP addresses of network adapters of the computer or corresponding DNS names. Server applications use IP address to which the *Administration Console* connects to distinguish local administration from remote administration. If remote administration is not enabled, the application accepts only connections to the `localhost`.

The *New Connection* caches a few servers which have been recently used. When connecting to the same server again, name or address of the server can simply be selected from a list (for this purpose, we recommend you to create a bookmark — then, connections will be faster and easier).

Username and Password

Username and password used for connection to a server application administration. User must possess the *Read/Write access* rights (for administration), or the *Read only access* rights (for configuration viewing).

The dialog also caches username used for the last connection.

Click *Connect* to establish connection with the selected server application. Upon successful connection and authentication, a corresponding administration module is opened and the main window of the*Administration Console* is closed.

Notes:

1. The network protocol used for communication between *Administration Console* and the server is independent from the operating system. This implies that for example *Kerio MailServer* at the server with *Mac OS* can be administered remotely from a workstation with *Windows*, etc.

2. To procure the best security possible, *Administration Console* test trustworthiness of the server's certificate upon each connection. For details, see chapter 3.3.

Creating a bookmark

To keep certain login data for repeated connections, click *Save As* before clicking on *Connect*. This button opens a dialog window for saving the bookmark.

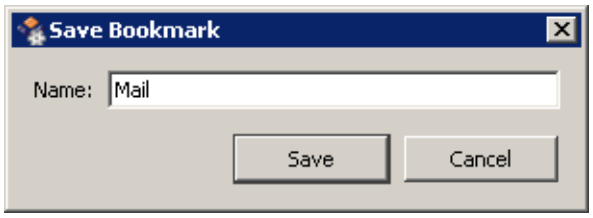

Figure 3.3 Saving a bookmark

Specify *Name* that will represent the bookmark in the *Administration Console's* main window. The name will be also used for the filename where the bookmark will be saved (see chapter 2).

Warning: If password is entered by the moment when the bookmark is saved, the password is also saved. Therefore, it is possible to protect bookmarks in *Administration Console* by password (for details, see chapter 3.4).

Bookmarks Context Menu

Right-click on a selected bookmark to open its context menu providing the following functions:

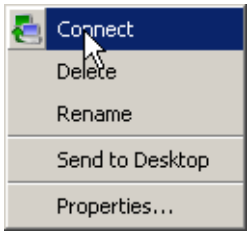

Figure 3.4 Bookmark context menu

- *Connect* — connection to a corresponding server application (double clicking or pressing *Enter* on the bookmark also establishes the connection).
- *Delete* — deletion of the selected bookmark. This action will physically remove a corresponding file from the disc (see chapter 2). Deleted bookmarks cannot be recovered unless there is a backup of the corresponding file available.
- *Rename* — bookmark's name modification. This can be also done by double-clicking on the bookmark's name (as well as the icon on the *Windows* desktop).
- *Send to Desktop* — use this option to create a link to the bookmark on the desktop. Bookmark files are matched with the *Administration Console* — double-clicking on the bookmark icon on the desktop runs a corresponding administration module and establishes connection to a corresponding server.

  Note: This function is available only under *Windows*.
- *Properties* — use this option to open the *Bookmark properties* dialog window. For detailed information on this dialog follow the instructions for the *New Connection* and the *Save Bookmark* dialogs described above.

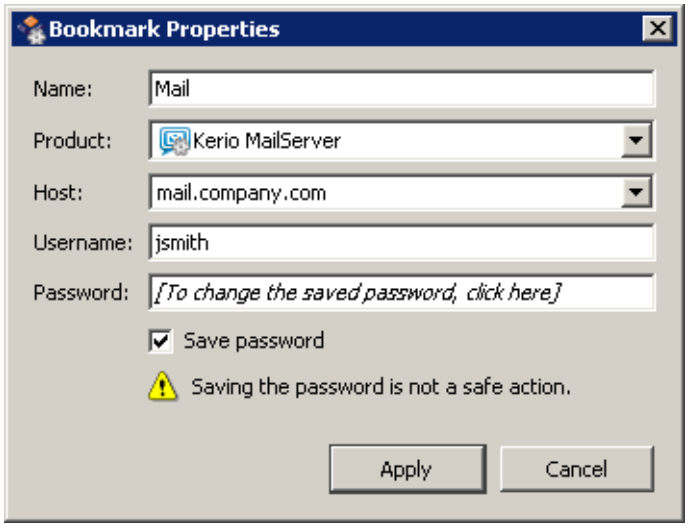

Figure 3.5 Bookmark configuration

3.3 Checking the server's identity

Within establishment of connection to a server application (*Kerio WinRoute Firewall* or *Kerio MailServer* — called simply *server* thereinafter), *Administration Console* (called simply *client* thereinafter) checks identity of the particular server. This security feature protects from so called "man-in-the-middle" attack type (the attacker pretends to be the destination server, captures client's login data and uses it to connect to the real server).

The server prooves its identity by an SSL certificate. The client compares so called certificate fingerprint with the fingerprint saved in its configuration file. If the fingerprints match each other, the connection is permitted automatically. Otherwise, intervention of the user is required.

Notes:

1. The check of the certificate is not applied to connections from the very host where the particular server application is installed (connection to `localhost`). In such cases the "man-in-the-middle" attack would be meaningless (the attacker might harvest fragile data much more simply).

2. Connection by *Administration Console* does not use the SSL certificate which is set for "client" services (web interfaces, etc.) in the server application; in such cases, a special self-generated certificate is used.

First connection to the server

Let us suppose that *Kerio WinRoute Firewall* has already been installed on `server.company.com`.[1] And at the very moment, you need to connect to this server from another host by using the *Administration Console* for the first time.

Fill in the login dialog (or create a bookmark — for details, see chapter 3.2). Upon clicking on the *Connect* button, a notice is displayed informing that the server identity could not be verified — see figure 3.6.

At this point, it is time to verify whether *Administration Console* connects to the correct server:

- In the *Server* textfield, check type of server application and IP address of the destination server.

  If the server is defined by name and its IP address does not agree, it is necessary to verify DNS record for the particular host name or to specify the server directly by the IP address. However, bear in mind that an incorrect IP address might point at an attack attempt (fake DNS record).

[1] The connection and identity check process is the same for *Kerio MailServer*.

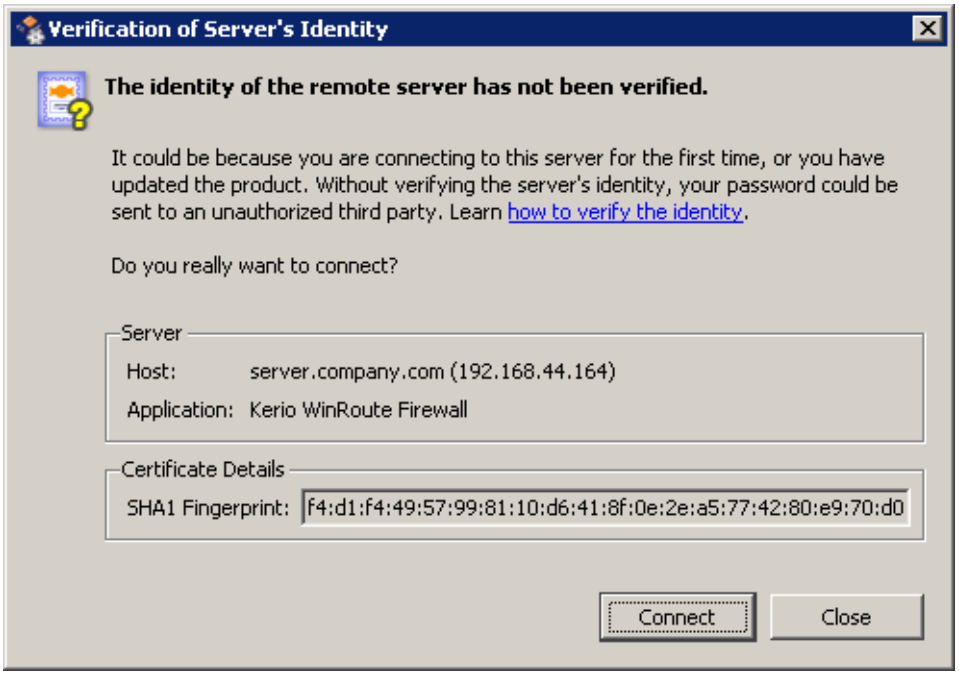

Figure 3.6 Verification of the server's identity — connection to a new server

Note: If the server is defined by an IP address, the DNS verification is meaningless and it is skipped.

If the server application type is not correct, it is recommended to check running server application on the particular server and attempt to connect to them locally.

- Compare the certificate's fingerprint in the *Certificate details* entry with the fingerprint of the particular server's certificate.

  If fingerprints do not match with each other, the certificate is fake.

  HINT: Certificate fingerprint can be saved to the clipboard and pasted to a file, email message, etc.

If the IP address, application type and certificate's fingerprint are correct, it is possible to connect securely to the server. Otherwise, use the *Close* button to deny the connection and try to find what caused the problems.

If the address and the server certificate do not change upon the next connection, *Administration Console* will consider the server as trustworthy and the identity verification dialog is not opened since then.

How to detect the server certificate's fingerprint?

A special, automatically generated SSL certificate is used to secure traffic between the server application and the *Administration Console*. This certificate is created upon the first startup of the server application after the installation or/and whenever the certificate cannot be found (it might have been removed, damaged, etc.). The certificate is saved in file `server.crt` under the `dbSSL` subdirectory of the installation directory of the server application (the exact path depends on application type and on the operating system).

The method used to detect the certificate's fingerprint depends on the operating system of the server:

Windows

By default, the server's certificate is stored under

`C:\Program Files\Kerio\WinRoute Firewall\dbSSL`

or

`C:\Program Files\Kerio\MailServer\dbSSL`

A dialog with certificate information is displayed upon opening of the certificate file (by double-clicking or by pressing the *Enter* key).

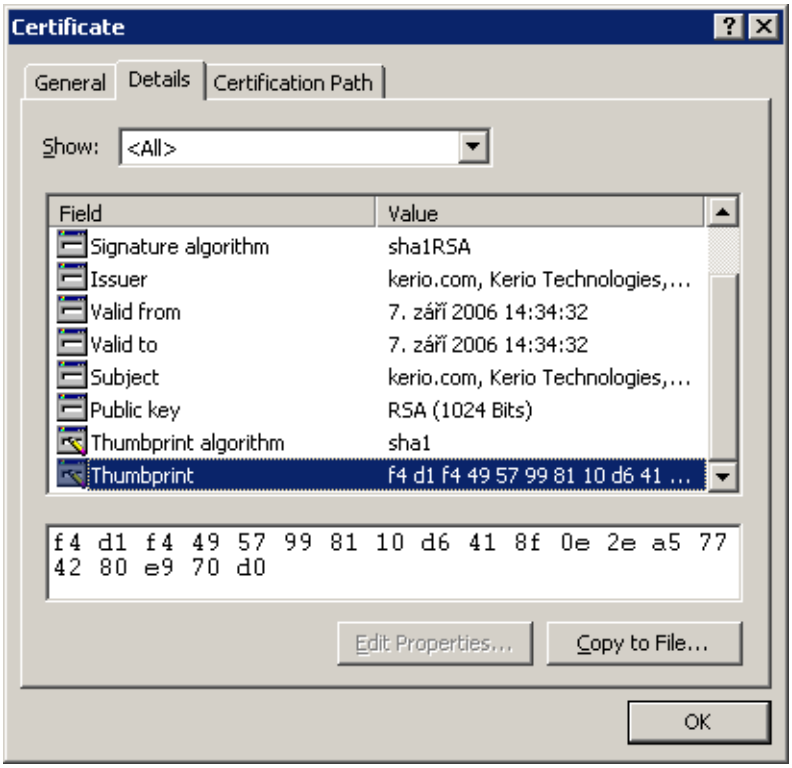

Figure 3.7 Viewing the server certificate's fingerprint on Windows

On the *Details* tab, look at the *Thumbprint* field.[2]. This field includes the certificate's fingerprint which can be saved to the clipboard and pasted to a file, email message, etc.

Linux and Mac OS X (Kerio MailServer only)

By default, the server's certificate is stored under

`/opt/kerio/mailserver/dbSSL` (Linux),

or

`/usr/local/kerio/mailserver/dbSSL` (Mac OS X).

To detect the certificate's fingerprint, use the `openssl` application (the *OpenSSL* package is required to be installed on the system).
In the console (terminal), open the directory which includes the `server.crt` file and enter the following command:

```
openssl x509 -in server.crt -noout -text -fingerprint -sha1
```

This command displays certificate information, providing the certificate's fingerprint on the last line:

```
SHA1 Fingerprint=F4:D1:F4:49:57:99:81:10:D6:41:8F:0E:2E:A5:
77:42:80:E9:70:D0
```

Warning: The information provided above apply to products *Kerio WinRoute Firewall* in versions *6.3.0* and higher and to *Kerio MailServer* in versions *6.4.0* and higher. Moreover, *Administration Console* is still compatible with older versions of these applications. If an appropriate administration module is installed (see chapter 2), it is possible to connect for example to administration of *Kerio WinRoute Firewall 6.2.0*. After the first connection (or upon the first change of the IP address, etc.), an alert is displayed informang that the identity has not been verified. However, in case of older versions of the server applications, it is not possible to detect fingerprint of the SSL certificate which is used for the administration. In this case, if you really wish to connect to the server, it is necessary to accept the connection without verification of the fingerprint.

Repeated connection to the same server

Unless the certificate's fingerprint or IP address of the server is changed, *Administration Console* verifies only through username and password during future connections. The verification of the certificate and the IP address of the server is hidden and the user cannot see it.

If the certificate's fingerprint has been changed, a warning is displayed — see figure 3.8.

[2] A proprietary name of the certificate's fingerprint.

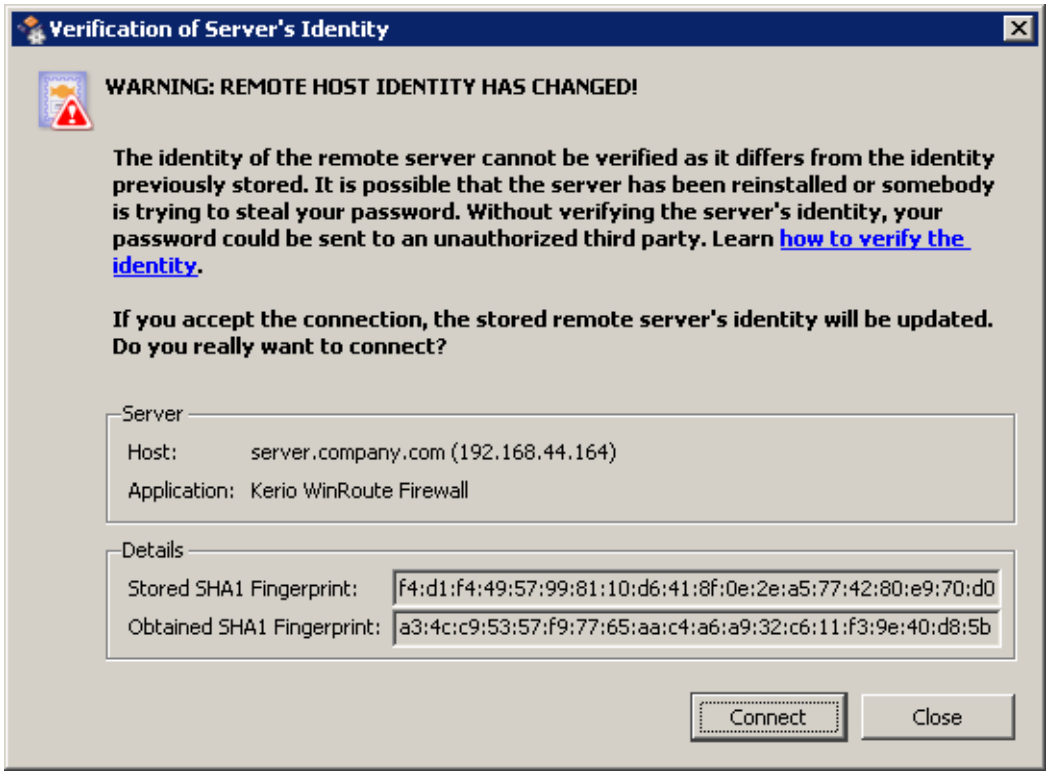

Figure 3.8 Verification of the server's identity — detection of the certificate change

Such a situation may occur when the server is reinstalled or when its certificate has been, by any reason, damaged or removed. In such a case, the server application has created a new certificate the fingerprint of which does not match with the fingerprint saved in the *Administration Console*. When we learn of such a change, verify the certificate's fingerprint applying the same mthod as for the forst connection (see above). If the new (accepted) fingerprint of the certificate matches with the server's certificate, connection can be allowed. In this case, the saved certificate's fingerprint is overwritten by the new fingerprint and no warning will be displayed upon future connections.

If the certificate on the server has not been changed, the situation might point at an attack (fake certificate). In such a case, use the *Close* button to deny the connection and try to find what caused the problems.

Note: When the server application is being upgraded, the original certificate is kept. In this case, the reinstallation means a brand new installation — for example when a new harddisk is introduced in the computer, etc.

Under certain conditions, IP address of the server can be changed (e.g. when the server is re-employed in another subnet). When IP address is changed, corresponding DNS records are usually also updated. This implies that the same DNS name is used during the following attempt for remote connection to the particular server application by

Administration Console, while the IP address will be different. There are two types of *Administration Console's* responses to change of the server IP address:

- If there is no record for the new IP address (and for the port of the particular server application) yet, *Administration Console* displays warning as in case of the first connection to a new server (see figure 3.6).
- If there is already a record for the new IP address and the port (i.e. *Administration Console* has already connected to the particular server application through the same IP address), the situation is considered and treated as a change of the server's identity (see figure 3.8).

In both cases, if the change of the IP address is desirable and cognizant, check the IP address and the (new) certificate's fingerprint and accept the connection upon acknowledging that no problem is found. If the IP address has not been changed, deny the connection and try to find the cause of the problem.

3.4 Password-protected bookmarks

Bookmarks in the *Administration Console* are used for simple and fast connection to a particular server. Therefore, they include complete login information, often including the password. If the *Administration Console's* host is accessed by an unauthorized person, bookmarks might be misused to get fragile information and perform undesirable configuration changes on the server.

The *Administration Console* therefore enables to protect bookmarks by password.

Bookmarks protection settings

In the main menu, select the *Tools / Protect Bookmarks with Password* option to set password parameters.

Figure 3.9 Setting password for bookmarks

By default (after installation of the *Administration Console*), no bookmarks are protected. Define a password and retype it for confirmation.

If bookmarks are already protected, the *Tools* menu includes the *Change Password of Protected Bookmarks* option instead. The *Old password* is required for personal authentication. The protection can be removed by leaving the *New password* and the *Confirm new password* entries blank.

Warning: It is strongly recommended to use the bookmark protection, especially if multiple persons use the *Administration Console's* host!

Using protected bookmarks

If bookmarks are password-protected, the password is required upon each startup of the *Administration Console*.

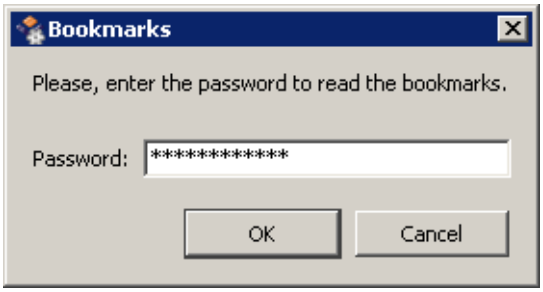

Figure 3.10 Setting password for bookmarks

If the correct password is entered, bookmarks can be handled in the standard way (see chapter 3.2). If the dialog is canceled (for example when the user does not know the password), only the *New connection* option can be used that enables connection to the server without the possibility to create bookmarks.

The password authentication dialog box can be opened again by the *Tools / Import bookmarks* option (the password is also required if there is an attempt to use a bookmark).

3.5 Connection Errors

This chapter provides description of the most frequent errors which are reported if connection to a server application fails.

Note: If an error which is not described here is reported, please contact *Kerio Technologies* technical support (all contacts can be found at `http://www.kerio.com/`).

Remote computer not found

This error is reported in case that the specified remote computer (server) could not be found (is not available).

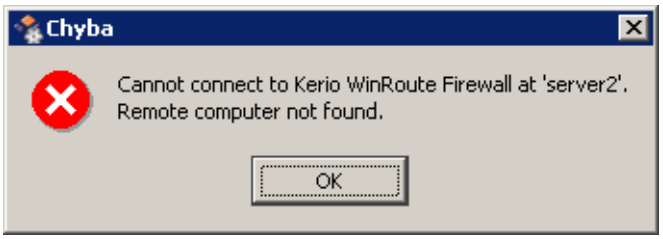

Figure 3.11 Connection failed: Server not found

Possible reasons of the error:

- Wrong specification of IP address or DNS name of the server .

  Make sure that you use a correct IP address or that the DNS name you use is still valid (e.g. using the `nslookup` system tool).

- Destination host is not available (e.g. for a network communication failure or because the traffic is blocked by a firewall).

  Test availability of the destination host by the `ping` command, or change your firewall settings.

Server application is not running

If the *Administration Console* cannot establish network connection to the server application on a corresponding computer, then the *Server application is not running* error is reported.

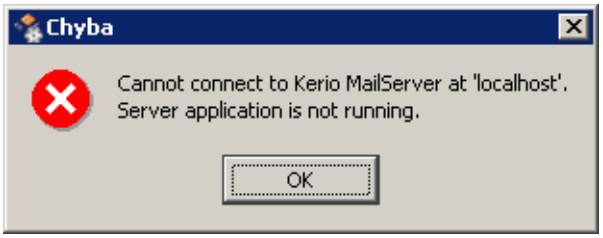

Figure 3.12 Connection failed: Server application is not running

Possible reasons of the error:

- Server application is not running.

  Check whether the *Kerio WinRoute Firewall* or the *Kerio WinRoute Firewall* service is running on the host you are connecting to.

- Connection to a corresponding application port cannot be established (the communication is blocked by a firewall).

  Try to use the `Telnet` command to establish connection with a particular port (see chapter 4) and change firewall configuration if necessary.+

User authentication failed

If the *Administration Console* establishes connection to the server successfully and there is a problem with user authentication, the *Authentication failed* error is reported.

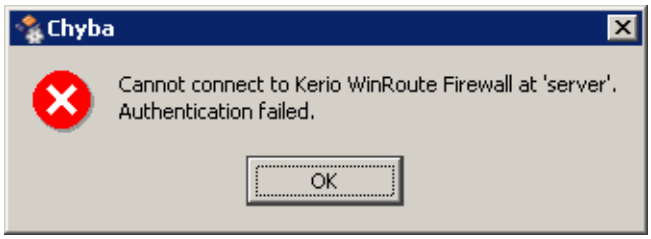

Figure 3.13 Connection failed: Authentication failed

Possible reasons of the error:

- Invalid username or password.

  Check whether your login data has been inserted correctly. If this error is arises when connecting through a bookmark, try to connect through *New Connection* by re-inserting all login data (for example, the user password could be changed and the bookmark may use an old password).

- Remote administration of the server application is disabled or it is available from a certain range of IP addresses only (your computer does not belong to this group). For details refer to a corresponding server application's user guide.

- User has not appropriate access rights.

  User account through which it is possible to connect must have the *Read/Write access* right (for administration), or the *Read only access* right (for configuration viewing).

- Authentication at the server failed.

An error occurred at the server that caused that the usual method of user authentication cannot be performed (e.g. in the *Active Directory*). For connection to the administration we recommend you to create a special user account in the internal user database (for details, see corresponding server application user guides).

Unsupported version of server

This error is reported in case that the *Administration Console* cannot find an administration module corresponding with the used version of server application (e.g. *Kerio WinRoute Firewall 6.1.x* is installed at the server, whereas the administration module is available for version *6.0.x* only).

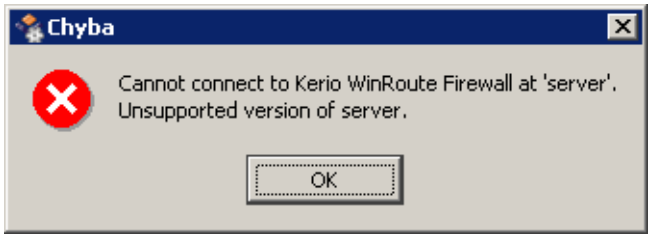

Figure 3.14 Connection failed: The server version is not supported

When this error is reported, install a corresponding administration module (or copy it into the `Admin` directory). It is highly recommended to use the same installation package from which the server application was installed.

3.6 Language preferences and splash screen settings

Use *Tools / Options* to open dialog where language preferences for the *Administration Console* and all its plug-ins can be set.

Figure 3.15 Setting language preferences

Use the *Show splash screen* option to enable/disable the *splash screen* shown after connection to a server application.

Check the *Always leave bookmarks window open* option if you want to leave the main *Administration Console* dialog window with the list of bookmarks open whenever connected to a selected server application. This function can be helpful for example when a user connects to various servers.

Note: Both described options are enabled by default.

Language preferences

Go to the *Preferred language* section to select a language which will be used for the *Administration Console* as well as for all administration modules.

Use the *Primary* entry to select a language which will be used. If the definition file of the selected primary language is not available (for example, it is missing or corrupted), the *Administration Console* tries to open the file which includes definitions for the *Alternate* language. If neither this file is available, the default language (English) of the *Administration Console* will be used.

The *Automatic* option sets language accordingly to the location where the program is used, if a corresponding language definition file is available.

Language definition files

The *Administration Console* (and the administration modules) includes only English version of the graphical user interface. Other languages must be included in so called definition files.

Location of definition files for individual operating systems is focused in chapter 2. The following files are required for any supported language:

`kadmin.<jazyk>.qm` — for the main window of the *Administration Console*

`mailadmin<XYY>.<jazyk>.qm` — for the *Kerio MailServer* administration module

`wradmin<VWW>.<jazyk>.qm` — for the *Kerio WinRoute Firewall's* administration module (only for *Windows*)

where

- the expression `<XYY>` represents major and minor number of version of the *Kerio MailServer* administration module
- the expression `<VWW>` represents major and minor number of version of the *Kerio WinRoute Firewall* administration module
- the `<language>` item consists of two characters which represent an abbreviation of a particular language (e.g. `fr` for French, `de` for German, etc.)

Note: If administration module for only one application has been installed, only language definition files for the *Administration Console* and for the particular module will be installed.

Example: Kerio WinRoute Firewall 6.1.5 and *Kerio MailServer 6.0.1* have been installed. The `kadmin.cs.qm`, `mailadmin600.cs.qm` and `wradmin601.cs.qm` definition files will be installed for Czech version.

3.7 Help (Windows)

On *Windows*, there are help files in the *HTML Help* format available in the *Administration Console* that can be used (`*.chm`) both for the main window of the *Administration Console* (the *Help / Contents* option in the main menu) and for both administration modules (the *Help / Administrators Guide* option in the main menu).

The installation packages include only English versions of the help files. However, help files in other languages are available at `http://www.kerio.com/`.

Location of help files is described thoroughly in chapter 2. The format of their names is as follows:

`kadmin.<jazyk>.chm` — help file for the main window of the *Administration Console*

`mailadmin<XYY>.<jazyk>.chm` — administrator guide for *Kerio MailServer*

`wradmin<VWW>.<jazyk>.chm` — administrator guide for *Kerio WinRoute Firewall*

where

- the expression `<XYY>` represents major and minor number of version of the *Kerio MailServer* administration module
- the expression `<VWW>` represents major and minor number of version of the *Kerio WinRoute Firewall* administration module
- the `<language>` item consists of two characters which represent an abbreviation of a particular language (e.g. `fr` for French, `de` for German, etc.)

First, the *Administration Console* (or an administration module) always searches for the help file in the language selected for the GUI (see chapter 3.6). If the file is not found, the help file in English will be searched. If neither the English version is found, the *Help / Contents* (in the main window) or the *Help / Administrator's Guide* (in the administration module's window) option is not available.

Note: The help is currently not available for *Linux* and *Mac OS*. The *Administration Console's* main menu or the administration module's menu does not include the options.

However, the manual in either *HTML* or *PDF* can be used for reference — there are no differences between individual format versions of the help/manual.

How to add a help file

Example: Suppose you want to add a French help file and French administrator guide for the *Kerio WinRoute Firewall 6.1.x* (for up-to-date version check the information provided at the welcome screen immediately after a successful login) into the *Administration Console*. Download corresponding guides in the *HTML Help* format from `http://www.kerio.com/` and save them to the `help` subdirectory (see above). The following files are available:

- a guide for the *Administration Console* (as `kadmin.cs.chm`)
- administrator guide for *Kerio WinRoute Firewall* (as `wradmin601.cs.chm`)

If we attempt to add while the *Administration Console* (or another administration module) is running, the following rules are applied:

- The help file for the *Administration Console* will be available upon the next startup of the *Administration Console* or when a new language version of the file has been enabled.
- Administrator guide for a corresponding application will be available upon the next connection to this application (upon the next startup of a corresponding administration module).

3.8 Importing old bookmarks

Older versions of the *Kerio Administration Console* (*1.x*, distributed along with *5.x* server products) followed a different method of bookmarks storing. The current version of the *Administration Console* (*2.x*) cannot use these bookmarks directly. However, corresponding login data may be imported and new bookmarks can be created out of the old ones.

To import and convert old bookmarks, use the *Tools / Import old bookmarks* option in the main menu of the *Administration Console*.

First, *Administration Console* searches a file which includes old bookmarks (`_admin.bkm`) in the home directory of the current user. If the file is found, the *Administration Console* checks whether it is encrypted and password-protected. If so, password is required.

The *Bookmark Import* dialog is opened upon a successful login.

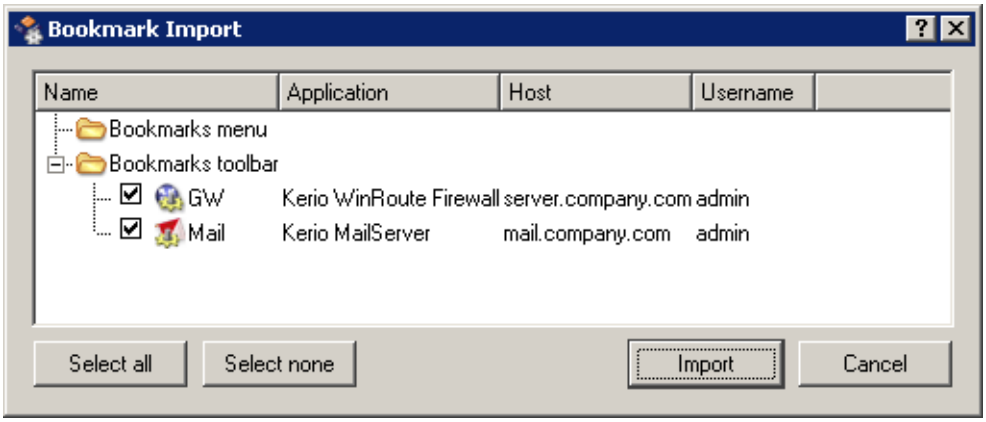

Figure 3.16 Importing old bookmarks

All bookmarks defined in the older version of the *Administration Console* are listed both in the list of bookmarks and on the toolbar. Select bookmarks to be exported to the new version and click on the*Import* button. If the process is completed successfully, imported bookmarks are added to the list in the main window of the *Administration Console*.

Note: You cannot connect to the server defined by an imported bookmark unless the corresponding server application has been updated to the version *6.x*. It is not possible to connect to previous versions (*5.x*).

Chapter 4

Network communication of the Administration Console

Brief description of network communication between the *Administration Console* and server applications will be provided in this chapter. This information may be helpful for example when a remote administration is performed and the server application is running behind a firewall where this communication must be allowed.

For this communication, TCP (transmission of configuration data) and UDP protocols (transmission of new log items from the server to the *Administration Console*) are used. Each server application uses one port number for connection to the administration (the term "application port" will be used from now on). At this port, the server listens for an incoming TCP connection and for an initiating UDP message (see below).

Kerio Technologies products use the following ports:

- `44333` — *Kerio WinRoute Firewall*
- `44337` — *Kerio MailServer*

Communication between the client and the server

Communication between the *Administration Console* (the term "client" will be used from now on) and a server application (the term "server" will be used from now on) is as follows:

1. The client establishes a TCP connection (through an encrypted channel) to corresponding application port at the server. Upon a successful authentication, so called connection identifier is provided by the server.
2. The client sends a UDP message including the connection identifier to the corresponding application port.
3. The server remembers the port from which the message with the connection ID was sent. This port will be used for delivery of new log items).
4. When the TCP connection is terminated (by logging out, by closing a client or a server, because of a network error, etc.), a corresponding connection identifier

is removed by both the server and the client. Any other UDP messages with this client port will be ignored.

Firewall configuration

This section provides firewall configuration hints for communication between the *Administration Console* and a server application in the following situations :

1. The server is running behind the firewall (in a local network or on the firewall host), the client is in the Internet

   A corresponding application port (44333 or 44337) for TCP and UDP protocols must be opened (mapped) at the firewall.

2. The client is behind the firewall, the server is in the Internet

   The firewall configuration must allow outgoing TCP connection and UDP communication at a corresponding application port.