Kerio Operator

Administrator’s Guide

Kerio Technologies

This guide provides detailed description on *Kerio Operator*, version *1.0*. All additional modifications and updates reserved.

For current versions of the product and related manuals, check

http://www.kerio.com/operator/download.

Information regarding registered trademarks and trademarks are provided in the appendix A.

Contents

Chapter 1

Introduction

Kerio Operator is a telephone exchange (PBX) for small and medium enterprises which enables you to make calls using the SIP protocol or standard digital telephony ISDN (PRI/BRI). Besides management of very calls, *Kerio Operator* allows to create conferences, manage queues of calls, use scripts of an automated operator as well as for example configure specific types of hardware IP telephone devices. In short, *Kerio Operator* is a complex solution for your Internet telephony.

You can get *Kerio Operator* either as a hardware device or as a software application.

Kerio Operator is based on the Asterisk open-source telephone PBX (for details, see the official website at http://www.asterisk.org/).

1.1 Additional documentation

In addition to this document (*Kerio Operator, Administrator's Guide*), the following documentation goes hand in hand with *Kerio Operator*:

- Kerio Operator, Step-By-Step Guide — this document focuses on installation and basic configuration of the *Kerio Operator* PBX.

- Kerio Operator Box, Installation Guide — this document focuses on installation of *Kerio Operator Box*.

- Kerio Operator, User's Guide — this document focuses on installation and configuration of software phones and the *Kerio MyPhone* interface.

Besides the documentation, you can also target various issues by referring to:

- The context help is built in the product (see chapter 3.3).

- Product forum — in this discussion, you can encounter experience and problems of other administrators using the same product. You may find a working solution for your issues here.

- Knowledge Base — here you can find a set of articles troubleshooting particular problems.

Chapter 2

Installation

The installation of *Kerio Operator* differs for:

- *Kerio Operator* — the software version available as an ISO image.
- *Kerio Operator Box* — the PBX on a special hardware.

2.1 Kerio Operator

To install *Kerio Operator*, you need a computer with the following minimum hardware configuration:

- CPU 1 GHz,
- 512 MB RAM,
- 8 GB free disk space,
- Ethernet card.

You obtain *Kerio Operator* as a standard ISO image which you need to burn on a CD. Boot from this CD and install the *Kerio Operator* operating system. The *Kerio Operator* PBX is also installed during the process.

2.1.1 Network Connection

After booting the system, a console with the IP address for *Kerio Operator* is displayed.

If you use a DHCP service on your network, *Kerio Operator* will be assigned an IP address automatically and will connect to the network. If you do not use or do not wish to use DHCP for *Kerio Operator*, you have to set the IP address manually.

The current network configuration is displayed (and can be changed) in the *Kerio Operator* console in section `Network Configuration`. To set a static network address:

1. Select the *Network Configuration* option in the console menu.
2. In the network interface in which the PBX should communicate, select the `Assign static IP address` option and enter the IP address, subnet mask and gateway and DNS server IP addresses.

If you know the IP address of *Kerio Operator*, you can use the web interface to connect to it and configure it (see chapter 3).

Warning:
Immediately after you connect *Kerio Operator* to the network, we recommend to read chapter 5 concerning the security measures. Meeting security principles for *Kerio Operator* operation is extremely important. If the PBX is not protected appropriately by a firewall and supporting security rules, your internal telephone extension can be misused which may result in unexpected financial costs.

2.2 Kerio Operator Box

Kerio Operator Box 1000 series is an appliance which includes:

- CPU Celeron 1,5 GHz,
- 2 GB RAM,
- 8 GB Industrial-Grade CompactFlash
- external source

Kerio Operator Box 3000 series is an appliance which includes:

- CPU Pentium Core Duo 2,4 GHz ,
- 2 GB RAM,
- 16 GB Industrial-Grade CompactFlash,
- Suitable for rack,
- 1 slot for a PCI card where you can optionally insert:
    - ISDN PRI (Primary Rate Interface) also know as T1 or E1 — Digium TE122 (1 PRI port),
    - ISDN BRI (Basic Rate Interface) — Digium B410P (4 BRI ports).

For detailed information on connecting the device into the network, see the Kerio Operator Box, Installation Guide manual.

2.2.1 Network Connection

Upon the first start, the appliance has a static IP address set to `10.10.10.1`. There are two ways to change the configuration:

- in the console — use an ethernet cable to connect to the console. In the console menu, select the *Network Configuration* option and chnage the configuration.
- in *Kerio Operator Web Administration* in section *System* — to connect to the interface (see chapter 3).

  To connect to *Kerio Operator*, set the following TCP/IP parameters on your computer:

  - IP address: `10.10.10.2`
  - Subnet mask: `255.255.255.0`

Note: To shut down the appliance:

1. Connect to *Kerio Operator* via the console and select the `Shutdown` command.
2. *Kerio Operator* série 1000 will shut down.
   Kerio Operator série 3000 will stop the server, however, the physical appliance stays switched on. Wait until you are not able to connect to *Kerio Operator* via *Kerio Operator Administration* and turn the appliance off using the *pwr* on the appliance.

Chapter 3

Interfaces for communication

Kerio Operator offers two web interfaces: for administrators (*Kerio Operator Administration*) and for users (*Kerio MyPhone*). We recommend the following browsers to connect to the interfaces:

- Firefox 3.0, 3.5 and 3.6
- Internet Explorer 7 and 8
- Safari 4 and 5

Web interface are currently localized into Czech and English. You can change the language in the top right corner in each interface. The default mode is set to automatically recognize your browser's language settings.

3.1 Kerio Operator Administration

In *Kerio Operator Administration*, the administrator can configure the *Kerio Operator* server. For security reasons, use only HTTPS to connect to the interface. The protocol uses a non-standard port 4201. However, *Kerio Operator's* IP address or DNS name entered in your browser's address bar is sufficient to connect to the interface. The protocol and the port are automatically redirected correctly. The URL has the following form:

```
https://Kerio.Operator.IP.Address:4021/admin
```

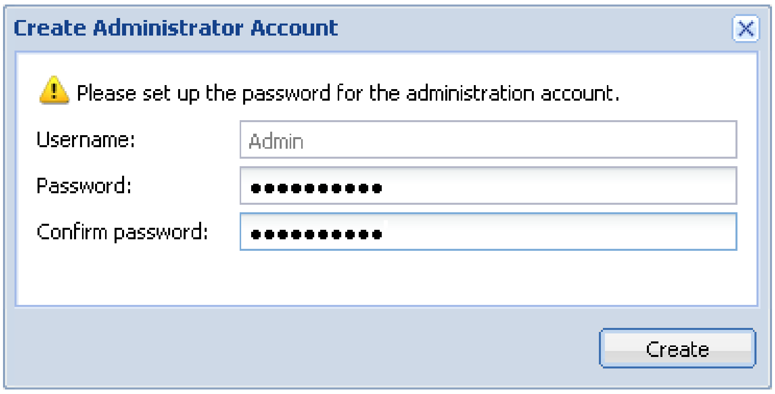
as you can see in the examples below:

```
https://192.168.10.1:4021/admin
```

If the URL is entered correctly, your browser displays a warning about a SSL certificate. After the installation, *Kerio Operator* creates a certificate which is not signed by a trusted certificate authority — it is a self-signed ceritiface (for more information, see chapter 19). Since you know the certificate can be trusted, you can add the security exception and continue to a login page.

A dialog is displayed where you can enter the login data for the first account in *Kerio Operator*. The name is automatically set to `Admin`, you enter a password. Remember the the information to login to *Kerio Operator Administration* (see figure 3.1).

Once you create the account, a login page for *Kerio Operator Administration* appears. Enter the username and password you created earlier (see figure 3.2).



Create Administrator Account

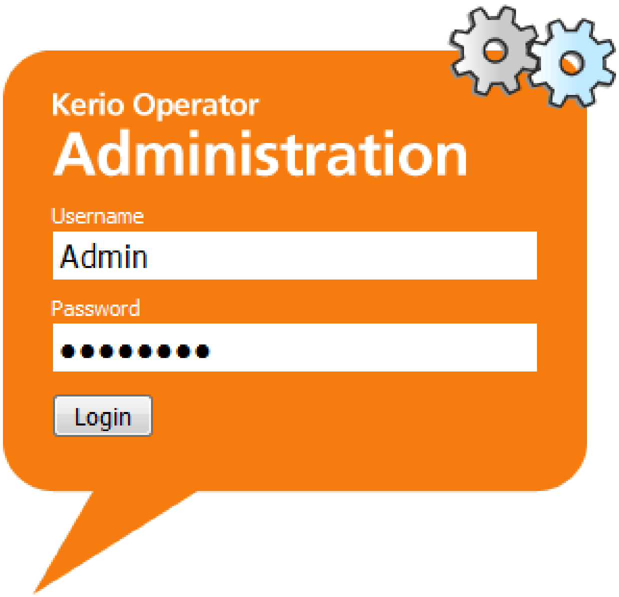
⚠ Please set up the password for the administration account.

Username: Admin

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

Figure 3.1 Creating administrator's account



Username: Admin

Password: ●●●●●●●●●

Figure 3.2 Connection to Kerio Operator

To change the password, use the following steps:

1. Login to *Kerio Operator* using the HTTPS protocol (for example `https://operator.company.com/admin`).

2. Go to section *Configuration* → *Users*.

3. In the user list, select the administrator account you under which you are logged in and double-click on it.

4. On the *General*, change the password. Repeat your new password to confirm the change.

3.2 Kerio MyPhone

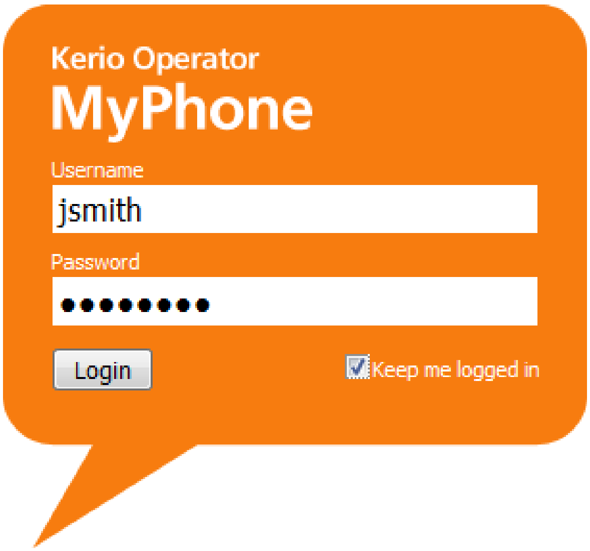
Kerio MyPhone interface allows the users to access

`http(s)://Kerio.Operator.IP.address`

or

`http(s)://Kerio.Operator.DNS.name`

If the URL is entered correctly, *Kerio MyPhone* login page is displayed (see figure 3.3).



Kerio Operator
MyPhone

Username: jsmith

Password: ●●●●●●●●

Figure 3.3 Connection to Kerio Operator

3.3 Context Help

The *Kerio Operator* web intereface includes a built-in context help. Use the context help especially when you are not sure what to enter in a field or whether to check an option.

The context help can be displayed by clicking on the question mark in the top right corner of the main window (figure 4.1) or a dialog (figure 6.7).

Chapter 4

Product Registration and Licensing

Once purchased, *Kerio Operator* must be registered. For registration of *Kerio Operator*, go to the administration interface (chapter 3.1) or to the official Kerio Technologies website.

If *Kerio Operator* is not registered, it behaves like a trial version. The trial version of *Kerio Operator* is not limited in functionality, it only expires after acertain period of time. After 30 days, Asterisk configuration files in *Kerio Operator* cannot be changed. Users will be able to make calls via *Kerio Operator* but no changes in *Kerio Operator Administration* will be allowed (for example, you will not be able to add new users and extensions).

This means that the trial version of *Kerio Operator* differs from the registered version only in time of functionality. This should be sufficient time (30 days) to test the product in the regular environment. It is not necessary to reinstall or reconfigure *Kerio Operator* after registration.

4.1 Product registration at the website

Web registration can be performed at the *Kerio Technologies* official website (https://secure.kerio.com/reg). This registration method is useful especially when *Kerio Operator* cannot access the Internet.

Against the registration, you will receive a licence key (the `licence.key` file including the corresponding certificate) which must be imported to *Kerio Operator*. For detailed information on the import of the license key, refer to chapter4.3.

Note: The trial version of *Kerio Operator* cannot be registered via the website.

4.2 Registration in the administration interface

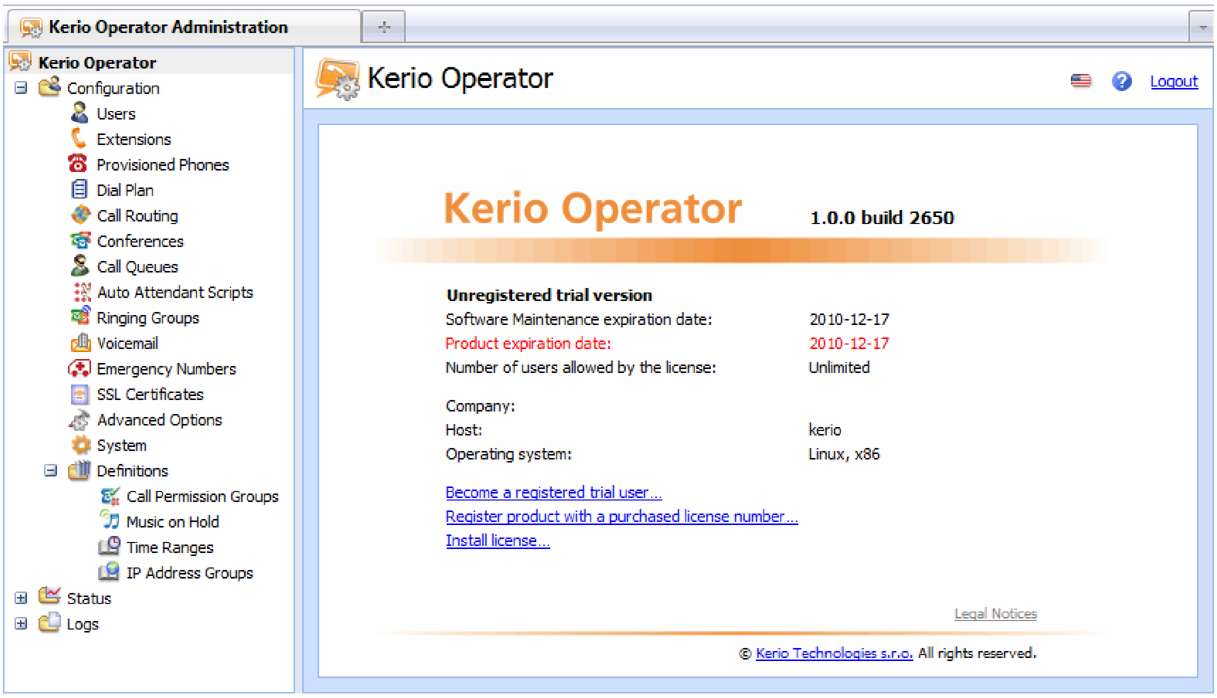
In *Kerio Operator Administration*, it is possible to make the registration using the link on the main page which is always displayed immediately after you login to *Kerio Operator Administration*.

> ***Warning:***
> If *Kerio Operator* is protected by a firewall, it is necessary to allow outgoing HTTPS traffic for *Kerio Operator* at port 443. Unless HTTPS traffic is allowed, *Kerio Operator* cannot use the port to connect to the *Kerio Technologies* registration server.

When installed, the product can be registered as trial or as a full version.

Why should I register the trial version?

The trial version is intended to allow the customer to become familiar with the product's features and configuration. Once you register the trial version, you will be provided free *Kerio Technologies* technical support during the entire trial period (up to 30 days).



Kerio Operator 1.0.0 build 2650

Unregistered trial version

Software Maintenance expiration date:	2010-12-17
Product expiration date:	2010-12-17
Number of users allowed by the license:	Unlimited
Company:	
Host:	kerio
Operating system:	Linux, x86

Become a registered trial user...
Register product with a purchased license number...
Install license...

Legal Notices

© Kerio Technologies s.r.o. All rights reserved.

Figure 4.1 Product registration

The trial version can be registered by clicking on *Become a registered trial user* on the product's main page (see figure 4.1). In the dialog box just opened, set the following parameters:

1. The *Trial Registration* dialog is opened where you enter the security code (CAPTCHA) in the field.
2. In the next step, enter information identifying you company and confirm you agree with the privacy policy terms.
3. In the following step, choose how many computers do you have in your company and how you learned of *Kerio Operator*.
4. In the last window, check correctness of the specified information. If there is no change to be made, click on *Finish* to send the registration.

Now, a special identification code called *Trial ID* gets generated. This ID is later required for contacting the technical support. After a successful registration, Trial ID can be found in the license information of the *Kerio Operator Administration*.

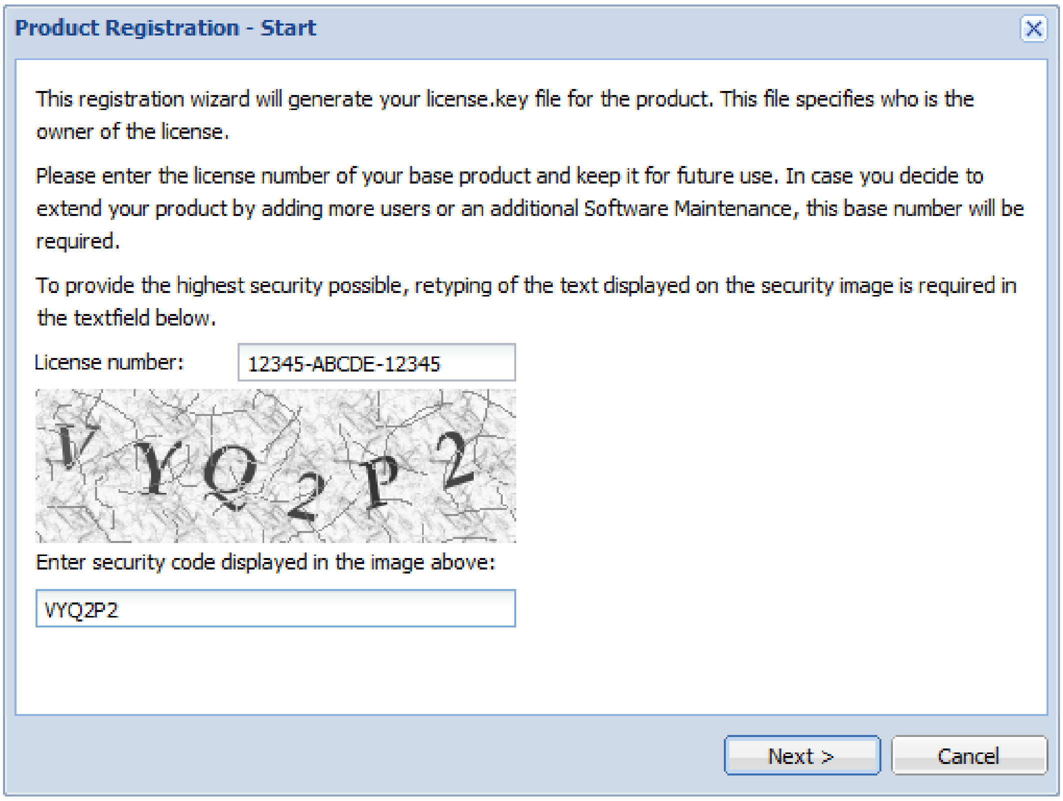
If the registration is completed successfully, a confirmation message will be sent to your email address provided.

Registration of full version

To run the process of full version registration, click on the *Register product with a purchased license number* link provided at the main page of the administration interface (see figure 4.1):

1. In step one, enter the license number you acquired upon purchasing the product and the security code (CAPTCHA) provided in the picture (see figure 4.2).

   Note: The code is not case-sensitive.

   Product Registration - Start

   This registration wizard will generate your license.key file for the product. This file specifies who is the owner of the license.

   Please enter the license number of your base product and keep it for future use. In case you decide to extend your product by adding more users or an additional Software Maintenance, this base number will be required.

   To provide the highest security possible, retyping of the text displayed on the security image is required in the textfield below.

   License number: 12345-ABCDE-12345

   Enter security code displayed in the image above:

   VYQ2P2

   Figure 4.2 License number

   Click *Next* to make *Kerio Operator* establish a connection to the registration server and check validity of the number entered. If the number is invalid, the registration cannot be completed.

2. In this dialog you can specify add-ons and/or *Software Maintenance*. If you have purchased only the base license so far (usually when registrating the product for the first time), skip this step.

3. At this page, registration information identifying the company (organization) to which the product is registered is required.

Note: The red entries marked with an asterisk are required, The other ones are optional.

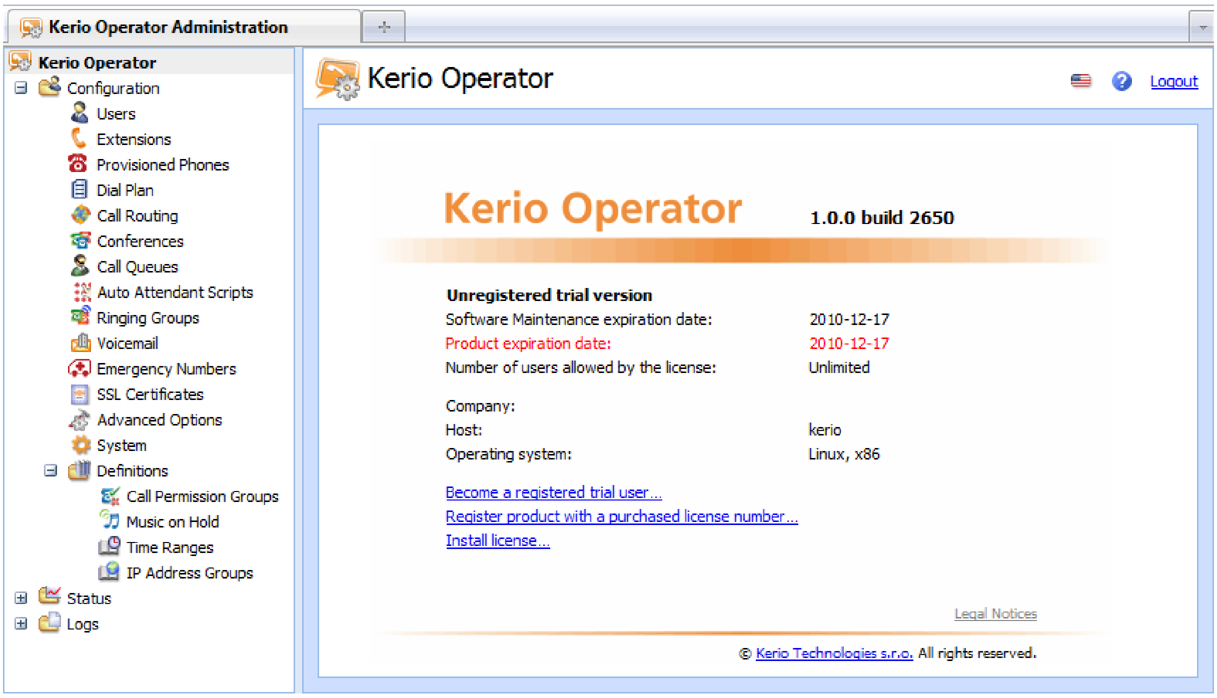
4. In the last dialog, the data specified in the wizard is summarized. Information of *Software Maintenance* expiration date is provided (the latest date when the product can be updated for free).

   Kerio Operator connects to the registration server, checks whether the data inserted is correct and downloads automatically the license key (digital certificate).

5. Click *Finish* to close the wizard.

4.3 License information and import of the license key

License information is provided at the main page of *Kerio Operator*. The *Kerio Operator* main page is opened upon each startup of the *Kerio Operator Administration*. It can be also displayed by clicking on *Kerio Operator* in the sections list provided in the tree.



Kerio Operator 1.0.0 build 2650

Unregistered trial version

Software Maintenance expiration date:	2010-12-17
Product expiration date:	2010-12-17
Number of users allowed by the license:	Unlimited
Company:	
Host:	kerio
Operating system:	Linux, x86

Become a registered trial user...
Register product with a purchased license number...
Install license...

Legal Notices

© Kerio Technologies s.r.o. All rights reserved.

Figure 4.3 Viewing license information

To run a full version of *Kerio Operator*, a license key is required. A license key is a special file that must be imported to the product. Two methods can be applied to obtain the key (depending on the type of the product's registration and on the fact whether the product was registered in time):

- The license key is imported automatically during the product's registration in the administration interface (see chapter 4.2).
- Import using the link on the main page — click on the *Install license* link (see figure 4.1). A standard file-opening dialog is displayed where the license key can be browsed and

imported. If the import is successful, information about the new license is provided at the main page.

- Adding the license key file in the `license` directory manually — it is possible to copy the `license.key` file manually to the `license` subdirectory under the directory where *Kerio Operator* is installed.

License ID
License number of the product.

Software Maintenance expiration date
The latest date when the product can be updated for free.

Product functionality expiration date
The date when the product expires and stops functioning (only for trial versions and special licenses).

Number of users allowed by the license
Number of users allowed by the license. Number in parenthesis refers to total number of lines/users using the *Kerio Operator*. The number includes lines and users created locally as well as mapped from a directory service.
If number of active users exceeds number of licensed users, the *Number of users allowed by the license* line is coloured by red to alert user.

Company
Name of the company (or a person) to which the product is registered.

Server
DNS name of the server with *Kerio Operator*.

Operational system
Operating system on which *Kerio Operator* is installed.

If the *New version available...* link is displayed in the introductory window when the console is started, click on the link and download a new version.

4.4 Licensing policy

Number of users is counted by extensions/users created in *Kerio Operator*.

In case of users mapped from the LDAP database of the directory service, all users created in this database are counted as individual extensions.

Software Maintenance

Software Maintenance and add-on licensing policies are described in detail at the *Kerio Technologies* webpage — http://www.kerio.com/support/software-maintenance/.

Chapter 5

Secure PBX Operation

It is necessary to make *Kerio Operator* as secure as possible:

- Make sure firewall is configured properly and communication is possible only among the necessary IP addresses and ports (the SIP service provider server and so on), especially if the PBX is operated in the Internet.
- Strong SIP passwords should be set (do not use dictionary words, they should have more then eight characters and the password should contain three types of characters — letters, numbers and special symbols).
- Communication in the internal firewall of the PBX should be limited. To configure it, go to *Kerio Operator Administration* section *Configuration → System → Firewall*. For detailed information on the configuration see chapter 22.2.
- We recommend using special rules to limit international calls to countries which you usually do not call or limit international calls for employees who are not expected to call abroad. To configure it, go to *Kerio Operator Administration* section *Configuration → Definitions → Call Permission Groups*. For detailed information on the configuration see chapter 23.2.

It is extremely important to follow the above-mentioned rules to avoid misuse of your PBX. Such a misuse might lead to harmful expenses.

5.1 LAN Firewall Configuration

Kerio Operator is usually installed in a local network behind a firewall. In addition to the PBX's configuration, it is also necessary to perform corresponding additional settings of the firewall.

If the PBX is to be accessible from the Internet, certain ports have to be opened (mapped) in the firewall. Each mapped port might introduce security problems. Therefore, map ports only for those services which you want to make available from the Internet.

Service (default port)	Outgoing connection	Incoming connection
SIP (5060)	allow	allow for SIP servers of your provider
IMAP (143)	allow	allow, if integration with *Kerio Connect* is enabled and there is a firewall between *Kerio Connect* and *Kerio Operator*.
LDAP (389)	allow	deny
LDAPS (636)	allow	allow, if you use mapping from *Active Directory* or *Open Directory* and there is a firewall between the directory service and *Kerio Operator*.
HTTP (80)	allow	deny
HTTPS (443)	allow	allow, if you wish users to be able to connect to *Kerio MyPhone* and *Kerio Operator Administration* from the Internet.

Table 5.1 Services to be allowed on the firewall

Chapter 6

SIP interface administration

To allow *Kerio Operator* to communicate with other SIP servers, it is necessary to configure a connection interface. The interface needs to be configured for both incoming and outgoiing calls. To configure the interfaces, go to *Configuration* → *Call routing* in *Kerio Operator Administration*. During the incoming calls configuration a route for outgoing calls is automatically configured.

Before you call your VoIP services provider, you must be sure what you expect from your phone network and how big and reliable it should be.

6.1 Interface for a SIP provider

If you acquired a number or a SIP trunk with an interval of phone numbers from you SIP provider, you can configure the interface to make calls from your internal network via your Internet provider. Before you configure an interface, you need the following:

- telephone number or numbers form your SIP provider,
- IP address or DNS name of SIP server and the port (usually 5060 for TCP and UDP) on which it communicates (you get the information from your provider),
- at least one internal extension defined in *Kerio Operator* (preferably an operator which will direct the calls, see section 9.1),
- username and password for authentication to the SIP server of the provider (you get the information from your provider).

If you have the above data available, you can configure the interface and conenct to your provider's SIP server.

1. In the administartion interface, go to section *Configuration* → *Call routing* and click on the *Add a SIP interface* button. This opens the configuration wizard.
2. Enter a name for the interface (it may be the name of the provider). The name cannot contain spaces, national and special characters and must be unique.
3. Select the *New provider* option. The configuration differs for one number, multiple numbers and a SIP trunk with an interval of phone numbers:

One number

1. If you acquired one phone number from your provider,enter the number in the *New provider → With external number* field (in a pattern supplied by your provider) and click on *Next*.
2. Select an extension for the provider who will direct all external calls made to the number from your provider to internal extensions created in *Kerio Operator*.
3. In the *Prefix to dial out* field, enter a prefix to be used for outgoing calls. The prefix is used by *Kerio Operator* to route calls to the SIP server of your provider.
4. Click on *Next*.
5. Enter data acquired from your provider (DNS name and port of the SIP server and username and password for authentication).
6. Check the *Must register with the Registrar or Proxy* option. The majority of providers requires registration upon the first connection to the SIP server.
7. If the user ID differs from the telephone number, type it in the user ID field.
8. Check the *Send the following external IP address in SIP registration* option only if *Kerio Operator* is behind a firewall which cannot overwrite private address of *Kerio Operator* to a public address. If this is the case, enter the public IP address of your firewall.

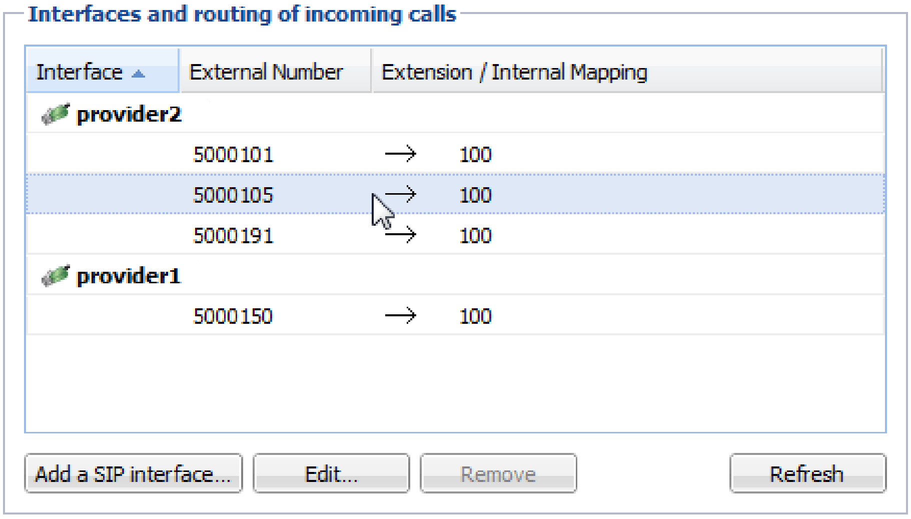
Multiple numbers

1. If you acquired multiple phone numbers from your provider,enter the numbers, separated by commas, in the *New provider → With external number* field (in a pattern supplied by your provider) and click on *Next*.
2. Select an extension for the provider who will direct all external calls made to the numbers from your provider to internal extensions created in *Kerio Operator*.
3. In the *Prefix to dial out* field, enter a prefix to be used for outgoing calls. The prefix is used by *Kerio Operator* to route calls to the SIP server of your provider.
4. Click on *Next*.
5. Enter data acquired from your provider (DNS name and port of the SIP server and username and password for authentication).
6. Check the *Must register with the Registrar or Proxy* option. The majority of providers requires registration upon the first connection to the SIP server.
7. If the user ID differs from the telephone number, type it in the user ID field.

8. Check the *Send the following external IP address in SIP registration* option only if *Kerio Operator* is behind a firewall which cannot overwrite private address of *Kerio Operator* to a public address. If this is the case, enter the public IP address of your firewall.

9. Save the settings.

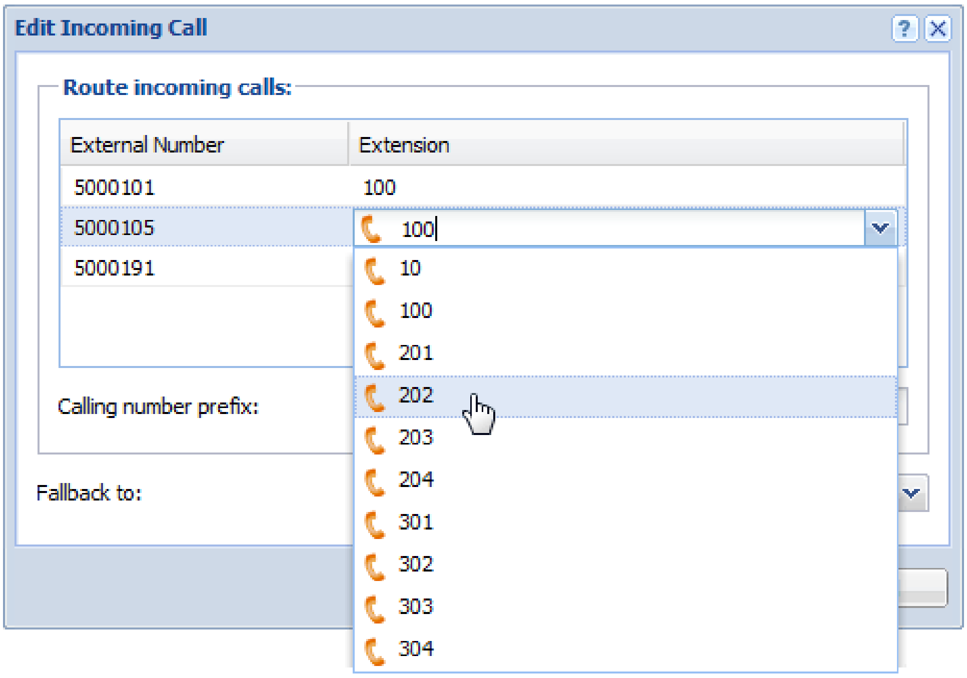
10. In section *Call routing → Interfaces and routing of incoming calls*, click on one of the lines with information about mapping of calls to the operator's extension (see figure 6.1).



Interface ▲	External Number	Extension / Internal Mapping
provider2		
	5000101	→ 100
	5000105	→ 100
	5000191	→ 100
provider1		
	5000150	→ 100

Figure 6.1 Mapping individual numbers to internal extensions of Kerio Operator

11. The *Edit Incoming Call* dialog is displayed (see figure 6.2). Click on a line in the *Extension* column to map external numbers to internal extensions.



Edit Incoming Call

Route incoming calls:

External Number	Extension
5000101	100
5000105	100
5000191	

Calling number prefix:

Fallback to:

Figure 6.2 Mapping individual numbers to internal extensions of Kerio Operator

Interval of numbers

1. If you acquired a SIP trunk with an interval of numbers from your provider, enter it in this specific pattern. Use X in place of the numbers to vary.

2. Click on *Next*.

3. Select an extension for the operator who will manually direct all external calls made to the numbers from your provider to internal extensions created in *Kerio Operator* unless mapping is configured.

4. In the *Prefix to dial out* field, enter a prefix to be used for outgoing calls. The prefix is used by *Kerio Operator* to route calls to the SIP server of your provider.

5. Click on *Next*.

6. Enter data acquired from your provider (DNS name and port of the SIP server and username and password for authentication).

7. Check the *Must register with the Registrar or Proxy* only if required by your provider. With large number intervals (so called “trunks”), providers usually do not require the registration. The registration is replaced by an IP address of *Kerio Operator*. The address must be fixed and the provider needs to know about its changes.

8. If the user ID differs from the telephone number, type it in the user ID field.

9. Check the *Send the following external IP address in SIP registration* option only if *Kerio Operator* is behind a firewall which cannot overwrite private address of *Kerio Operator* to a public address. If this is the case, enter the public IP address of your firewall.

10. Click *OK* to confirm settings.

11. Next, create a rewriting rule for correct mapping of numbers to internal user extensions. See section 6.3 for more details.

6.2 Interface for a second SIP server

If you wish to configure an interface for communication with another SIP server, follow these steps:

1. In the administartion interface, go to section *Configuration* → *Call routing* and click on the *Add a SIP interface* button. This opens the configuration wizard.

2. Enter a name for the interface (it may be the name of the server). The name cannot contain spaces, national and special characters and must be unique.

3. Select the *Link to another PBX* option and click on *Next*.

4. Enter a prefix for outgoing calls. The prefix tells *Kerio Operator* to which interface the call should be redirected. If you enter 3 (the second server uses extensions 3XX), all the numbers with prefix 3 will be directed to this server.

5. Click on *Next*.

6. In the *Hostname or IP address* and *Port number* filed, enter the DNS name or address of the second SIP server and the port on which it comunicates.

7. If the server requires authentication, enter valid data in the *Username* and *Password* field.

8. If the server requires registration,check the *Must register with the Registrar or Proxy* option.

9. If the user ID differs from the telephone number, type it in the user ID field.

10. If the first SIP server is behind firewall, check this option and enter the public address of the firewall in the IP address field.

11. Click *OK* to confirm settings.

12. Next, create a rewriting rule for correct mapping of numbers to internal user extensions. See section 6.3 for more details.

6.3 Overwrite rules

Rewriting rules ensure correct mapping of external and internal numbers in *Kerio Operator*.

Generally, an overwrite rule can strip first `0` to `N` digits from the number (the number may be reduced to an empty string) and then add other digits to the number. Overall, the overwrite rule allows to modify the left part of the number as needed by cutting or extending the number and/or replacing the ciphers in the beginning of the number string. See the example in figure 6.3.

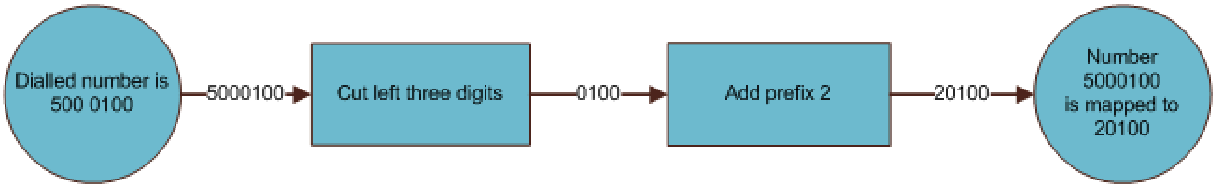


Figure 6.3 Overwrite rules for number 123456789

The following example shows the necessity and profitability of number rewriting (see figure 6.4):

1. You acquired 1000 phone extensions from your provider (800225XXX, or 800225000 — 800225999). You need to map these external numbers 800225XXX 1:1 to your internal extensions XXX.

2. For incoming calls, you want to add a prefix (9 in our example) to calling numbers so that it is easy for your users to dial back.

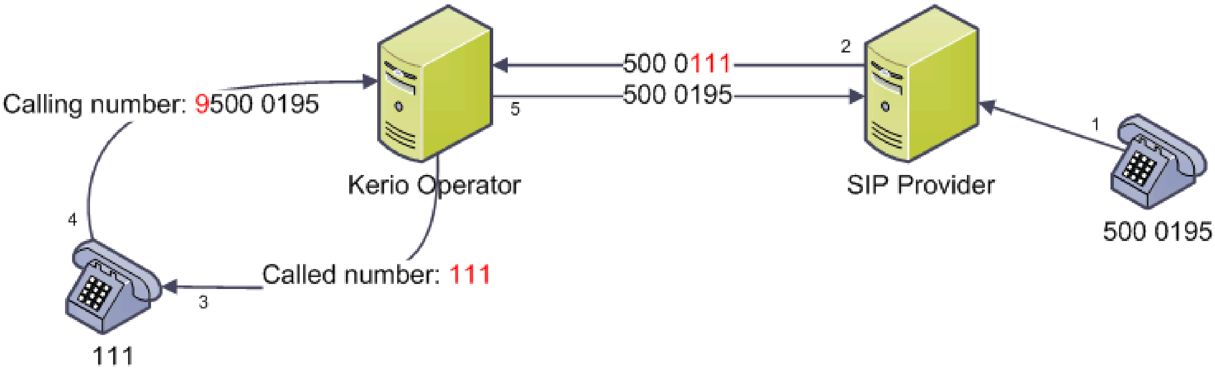
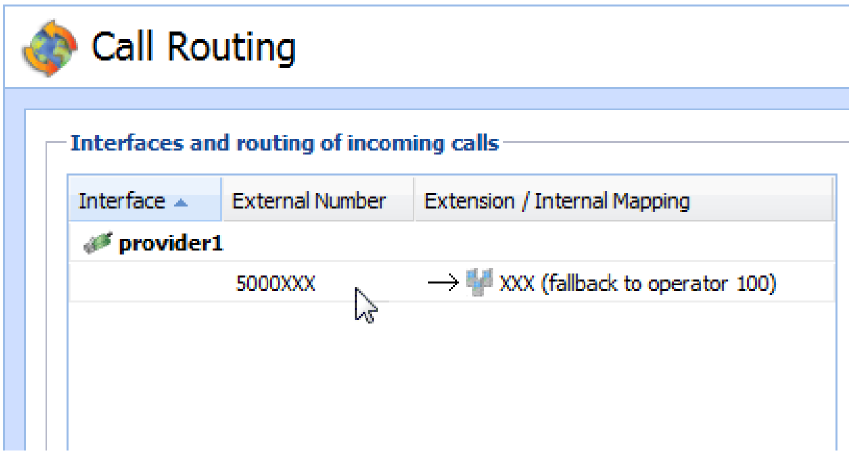


Figure 6.4 Incoming and answer call (read from right to left)

To achieve this, it is necessary to modify the rule for incoming calls on the interface (`provider1` in figure 6.5):

1. In the administration interface in section *Call Routing*, double-click on the routing rule for the interface of the SIP service provider (see figure 6.5).



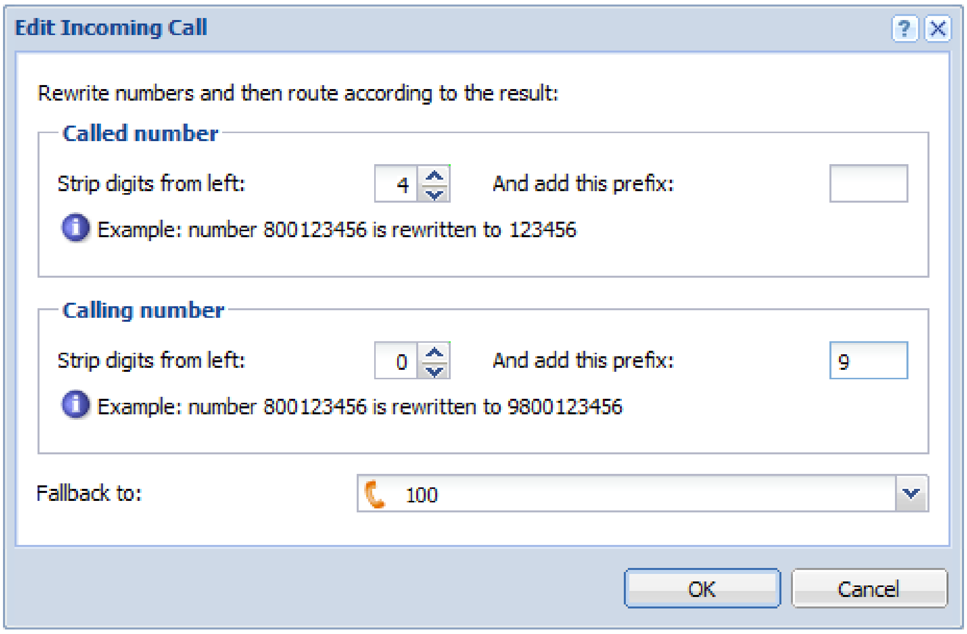
Call Routing

Interfaces and routing of incoming calls

Interface ▲	External Number	Extension / Internal Mapping
provider1		
	5000XXX	→ XXX (fallback to operator 100)

Figure 6.5 Rule for interface provider1

2. This displays the *Edit incoming Call* dialog. Modify the called number so that only the extension remains. Strip first 6 ciphers from left (800225 in our example which leaves extension 111). No prefix is necessary.



Edit Incoming Call

Rewrite numbers and then route according to the result:

Called number

Strip digits from left: 4 And add this prefix:

Example: number 800123456 is rewritten to 123456

Calling number

Strip digits from left: 0 And add this prefix: 9

Example: number 800123456 is rewritten to 9800123456

Fallback to: 100

Figure 6.6 Rule for interface provider1

3. Do not strip any ciphers from the caller's number and add prefix 9 from left.

Note: This setting applies to incoming calls. Incoming calls are such calls when someone from the external telephone network calls the internal extension of *Kerio Operator*. Naturally, there are also rewriting rules for outgoing calls. They are not described in our example because the initial settings usually suffice.
If you wish to understand the procedure, see section 7.3 with rewriting rules for outgoing calls for traditional telephone interface.

6.4 Setting Data Stream Codec

When calling, human voice is transformed to data stream and this stream is compressed to size small enough to go through internet lines. Various codecs (COder-DECoder) can be used for compression and transmission of data streams. When a certain codec is used for encoding a data stream, the recipient needs to have the same codec available to decode this data stream. *Kerio Operator* includes several codecs in order to meet various requirements of all the SIP clients and servers to encode and decode data steams without any problems.

Standard codecs in VoIP telephony are in particular: G.711 A-law and G.711 U-law. We recommend to keep these two codecs active.

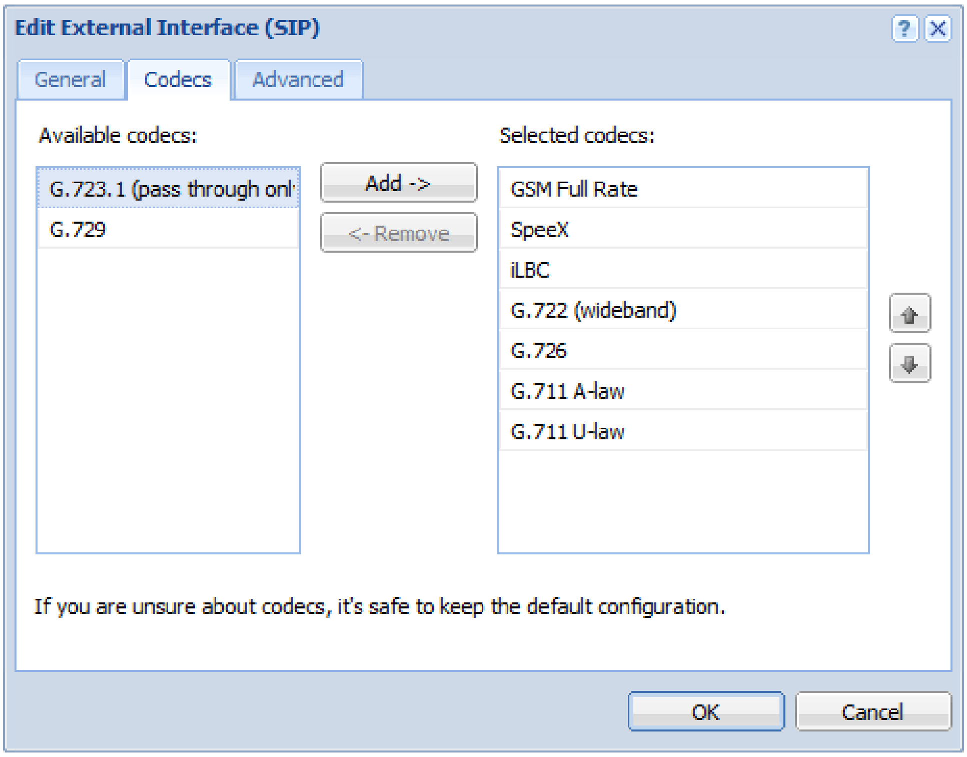
If your phone uses another codec for encoding data streams, follow the instructions:

Add new codec

To add a new codec:

1. Go to section *Call routing* in the administration interface and click on the interface for which you wish to use the codec.

2. In the *Edit external interface* dialog, go to tab *Codecs* (see figure 6.7).



Available codecs:

G.723.1 (pass through onl

G.729

Selected codecs:

GSM Full Rate

SpeeX

iLBC

G.722 (wideband)

G.726

G.711 A-law

G.711 U-law

If you are unsure about codecs, it's safe to keep the default configuration.

Figure 6.7 Interface for incoming calls → Codecs tab

3. In the *Available codecs* section, select the codec you wish to use and click on *Add* to move it to section *Selected codecs*.

4. Codecs are applied in their order, one by one. If you wish a particular codec to be used as default, select it and use the arrow button to move it to the top.

6.5 Removing interfaces

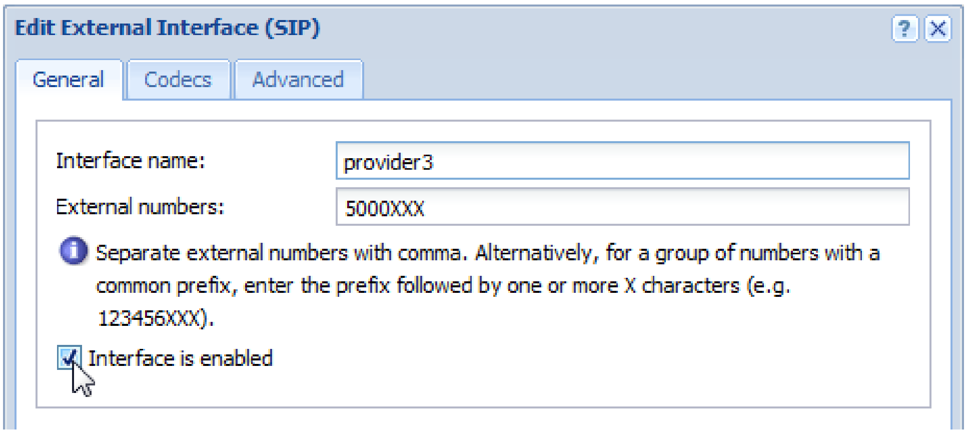
Any configured interface can be deleted. You can delete it temporarily or permanently.

Disabling Interface Temporarily

1. In the administration interface, open the *Call Routing* section.

2. Double-click on the interface for incoming calls which you wish to delete.

3. Uncheck the *Interface is enabled* option (see figure 6.8).



Edit External Interface (SIP)

Interface name: provider3

External numbers: 5000XXX

Separate external numbers with comma. Alternatively, for a group of numbers with a common prefix, enter the prefix followed by one or more X characters (e.g. 123456XXX).

☑ Interface is enabled

Figure 6.8 Block interface

Removing Interface

1. In the administration interface, open the *Call Routing* section.

2. In the outgoing calls section, remove all routes configured for the interface which you wish to delete.

3. Go to the incoming calls section, select the interface and click the *Remove* button to delete it.

6.6 Creating Alternative Connection for Route Backup

If you wish to backup your connection to the external network, you have to ensure connection with another (backup) SIP server or another phone extension (PRI/BRI). You may use a backup server of your VoIP service provider or you may choose another provider.

If you have a backup server, go to section *Configuration* → *Call routing* and:

1. Create new interface for incoming calls for the backup server (see section 6.1).

2. Go to section *Routing of outgoing calls* and double-click on the main interface (usually interface 0 in Europe or 9 in the USA). This opens the *Edit Outbound Route* dialog.

3. In table *Use the following external interfaces*, add your backup provider.

Chapter 7

Traditional Telephone Interface Administration

Kerio Operator allows you to use, apart from the communication over the SIP protocol, also the analog telephony. You need to acquire a PRI or BRI card and connect it. You can use the PRI or BRI card distributed with *Kerio Operator Box* series 3000 or use your own card and connect it to your *Kerio Operator* server.

If you have the card, create a connection interface similar to the interface for SIP server conenction. The interface needs to be configured for both incoming and outgoiing calls.

Before you call your telephone provider, you must be sure what you expect from your phone network and how big and reliable it should be:

- PRI card — the number of concurrent calls vary depending on whether you have contract with an american or european provider.
    - T (used in the USA) — allows 23 concurrent calls.
    - E1 (used in the EU) — allows 30 concurrent calls.
- BRI card — has 4 ports. Each port can operate two concurrent calls.

7.1 Configuring PRI/BRI interface for communication with the provider

If you acquired a number or a SIP trunk with an interval of phone numbers from your telephone provider, you can configure the interface to make calls from your internal network to an external network via your provider. Before you configure an interface, you need the following:

- telephone number or numbers form your telephone provider,
- ISDN type which is used for communication (it usually differs according to your location, for example, EuroISDN for the EU, Nation ISDN Type 2 for the USA and so on),
- whether your provider's PBX requires overlap dialing (see section 7.4),
- information whether PBX sends or requires telephone numbers whole or in the contracted form (see section 7.3),
- at least one internal extension defined in *Kerio Operator* (preferably an operator which will direct the calls, see section 9.1).

If you have the above mentioned information avalaible and at least one internal extension defined, you may configure the interface:

1. In the administration interface, go to section *Configuration → Call Routing*. If the PRI card is installed correctly, the *Interface and routing of incoming calls* table shows one traditional telephone interface.

   If the BRI card is installed correctly, the *Interface and routing of incoming calls* table shows 4 interfaces (one for each of the four ports).

2. Double-click on an unconfigured interface. This opens the configuration wizard.

3. Enter a name for the interface (it may be the name of the provider). The name cannot contain spaces, national and special characters and must be unique.

4. Select the *New provider* option. The configuration differs for one number, multiple numbers and a SIP trunk with an interval of phone numbers:

One number

1. Enter the number in the *New provider → With external number* field (in a pattern supplied by your provider) and click on *Next*.

2. Select an extension for the provider who will direct all external calls made to the number from your provider to internal extensions created in *Kerio Operator*.

3. In the *Prefix to dial out* field, enter a prefix to be used for outgoing calls. The prefix is used by *Kerio Operator* to route calls to the echange of your telephone provider.

4. Click on *Next*.

5. In the dialog, select the PBX type.

   - if you are in the EU, select the EuroISDN option,

   - if you are in the USA, select the National ISDN Type 2 option,

Multiple numbers

1. If you acquired multiple phone numbers from your provider,enter the numbers, separated by commas, in the *New provider → With external number* field (in a pattern supplied by your provider) and click on *Next*.

2. Select an extension for the provider who will direct all external calls made to the numbers from your provider to internal extensions created in *Kerio Operator*.

3. In the *Prefix to dial out* field, enter a prefix to be used for outgoing calls. The prefix is used by *Kerio Operator* to route calls to the PBX of your telephone provider.
4. Click on *Next*.
5. In the dialog, select the PBX type.
    - if you are in the EU, select the EuroISDN option,
    - if you are in the USA, select the National ISDN Type 2 option,
6. Save the settings.
7. In section *Call routing → Interfaces and routing of incoming calls*, click on one of the lines with information about mapping of calls to the operator's extension (see figure 6.2).
8. The *Edit Incoming Call* dialog is displayed (see figure 6.2). Click on a line in the *Extension* column to map external numbers to internal extensions.

Interval of numbers

1. If you acquired a SIP trunk with an interval of numbers from your provider, enter it in the *New provider → With an external number* field in a pattern supplied by your provider. Use X in place of the numbers to vary.
2. Click on *Next*.
3. Select an extension for the operator who will manually direct all external calls made to the numbers from your provider to internal extensions created in *Kerio Operator* unless mapping is configured.
4. In the *Prefix to dial out* field, enter a prefix to be used for outgoing calls. The prefix is used by *Kerio Operator* to route calls to the PBX of your telephone provider.
5. Click on *Next*.
6. In the dialog, select the PBX type.
    - if you are in the EU, select the EuroISDN option,
    - if you are in the USA, select the National ISDN Type 2 option,
7. Click *OK* to confirm settings.
8. Next, create a rewriting rule for correct mapping of numbers to internal user extensions. See section 7.3 for more details.

7.2 Configuring PRI/BRI interface for cummincation with another PBX

If you wish to configure an interface for communication with another PBX, follow these steps:

1. In the administartion interface, go to section *Configuration* → *Call routing* and double-click on the traditional telephone interface. This opens the configuration wizard.
2. Enter a name for the interface (it may be the name of the server). The name cannot contain spaces, national and special characters and must be unique.
3. Select the *Link to another PBX* option and click on *Next*.
4. Enter a prefix for outgoing calls. The prefix tells *Kerio Operator* to which interface the call should be redirected. If you enter 3 (the second server uses extensions 3XX), all the numbers with prefix 3 will be directed to this PBX.
5. Click on *Next*.
6. In the displayed dialog, select a PBX type, depending on the type used by the other PBX.
7. Click *OK* to confirm settings.
8. Next, create a rewriting rule for correct mapping of numbers to internal user extensions. See section 7.3 for more details.

7.3 Configuring Rewriting Rules

Rewriting rules ensure correct mapping of external and internal numbers in *Kerio Operator*. For general information about the function of rewriting rules see section 6.3 with description of rewriting rules for SIP interface. Analog interfaces use the same principles and, in addition, it is necessary to strip digits in numbers according to the needs of your telephone provider.

Telephone provider may send the callee's number whole or in the shortened form (usually last 4 digits) which suffice to recognize the correct extension. Similarly, the provider may also require whole numbers or numbers in the shortened form (usually last 4 digits). Request this information from your provider before you start interface configuration.

See the following example of rewriting rules:

- Company acquired 100 phone numbers from their telephone provider (a range of numbers 55501XX).
- For incoming calls, the provider strips the callee's number to last four digits (the number looks like this:01XX).
- For outgoing calls, the provider requires the caller's number in a shortened form (last 4 digits).

- Internal extension which will be bound to numbers from the acquired range of numbers have format 2XX.
- Prefix for outgoing calls is 9.

Rewriting rules are configured separately for incoming and outgoing calls.

Incoming Calls

Figure 7.1 shows what happens when a telephone with number 5550399 calls from the external to a company's telephone with number 5550101. Proceed from digit 1 from right.

1. After dialing a number, the call is automatically directed to a telephone provider based on the number's prefix.
2. Next, the number is identified by the telephone provider, stripped to the last four digits and sent to the *Kerio Operator* PBX.
3. According to the rewriting rule, the number is then stripped from left to 2 digits and prefix 2 is added from left. *Kerio Operator* now works with internal extension 201 and the call is successfully connected.
4. There may arrise a situation where user on extension 201 does not answer the call but wants to call back later. For that reason, it is necessary to define a back-call rule. To achieve this, add a prefix for calling to external network (otherwise, back-call will fail at the outgoing call interface).

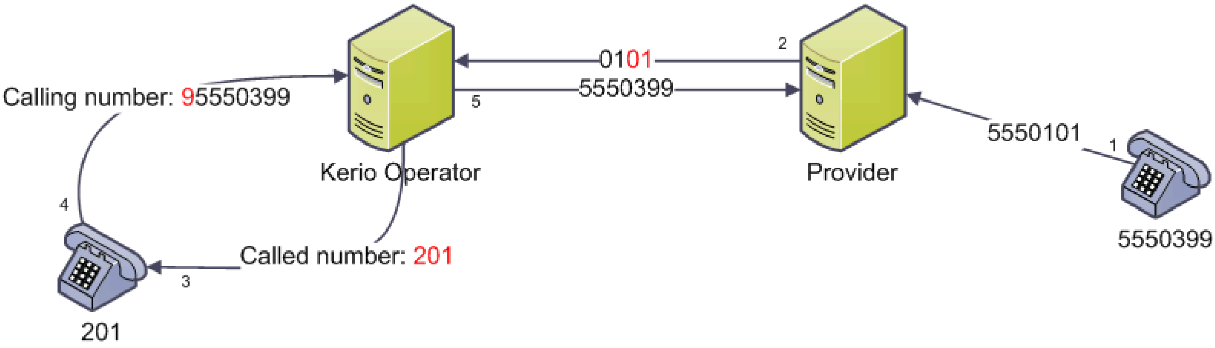
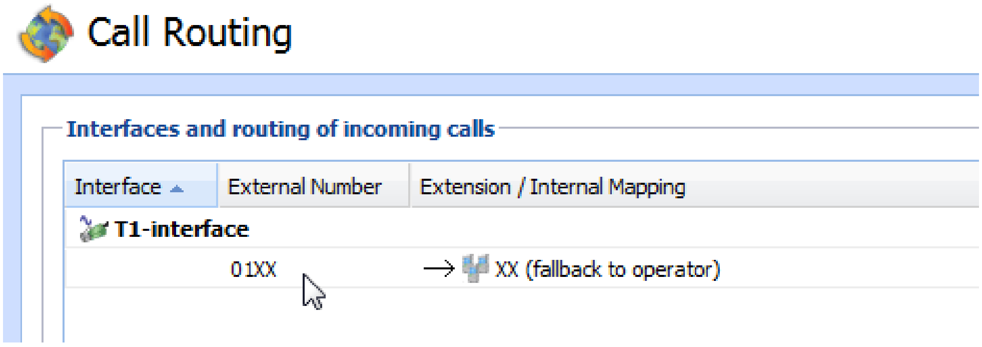


Figure 7.1 Incoming and answer call (read from right to left)

Make the following settings to ensure the above mentioned interface behavior:

1. Go to *Kerio Operator Administration* section *Call Routing* and double-click the routing rule for the traditional telephone interface (see figure 7.2).



Call Routing

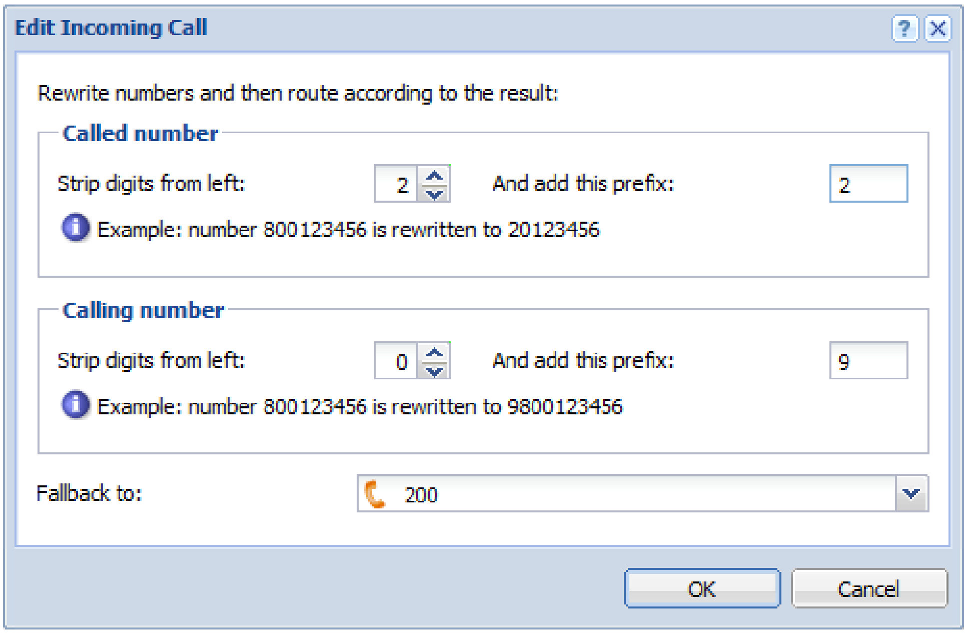
Interfaces and routing of incoming calls

Interface ▲	External Number	Extension / Internal Mapping
T1-interface		
	01XX	→ XX (fallback to operator)

Figure 7.2 Rule for traditional telephone interface T1

2. This opens the *Edit Incoming Call* dialog. Beer in mind that only the last 4 digits are included in the string.

   Strip the first two digits from left. Add prefix 2 to the stripped number of two digits (see figure 7.3). This modification provided the final format of the internal extension (2XX).



Edit Incoming Call

Rewrite numbers and then route according to the result:

Called number

Strip digits from left: 2 And add this prefix: 2

Example: number 800123456 is rewritten to 20123456

Calling number

Strip digits from left: 0 And add this prefix: 9

Example: number 800123456 is rewritten to 9800123456

Fallback to: 200

Figure 7.3 Rule for traditional telephone interface T1

3. We do not strip the digits in the calling number but we add prefix 9 from left (see figure 7.3).

Outgoing calls

Rewriting rules are also configured for the outgoing calls. These are calls which are initiated on an internal extension in *Kerio Operator* and are directed to an external telephone network.

We use the same example as in configuration of rewriting rules for incoming calls. The configuration will solve the following problems:

- Strip the prefix for outbound calls that determines to which interface (provider) the call will be directed (see figure 7.4).
- Adapt the internal extension which you call from in a way that the number meets the call criteria of your provider (see figure 7.5).

This scheme best describes the whole procedure 7.4 (follow the numbering):

1. User with extension 201 calls number 5550199. Since the called number is external, we must use prefix for calling external telephone network, which is in out case number 9. Final format dialed by the user will be 95550199.
2. *Kerio Operator* uses the rewriting rule and removes prefix 9.
3. The telephone provider directs the call to the called number.

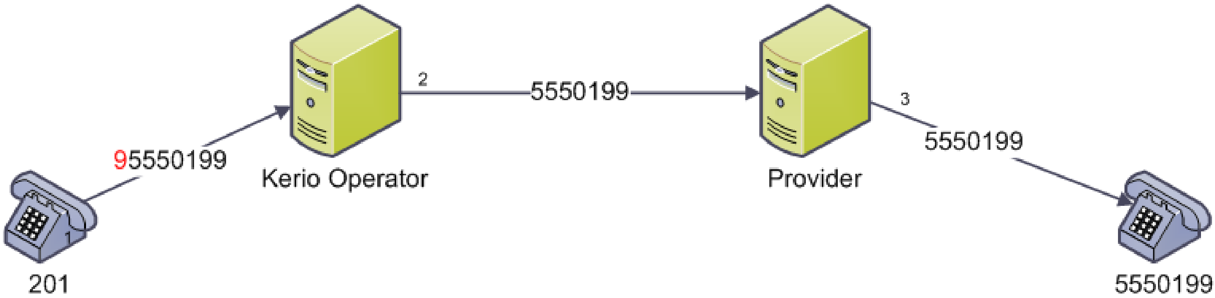


Figure 7.4 Scheme describing how to adapt called number

The following example shows the way the internal extension changes during outgoing calls (see figure 7.5):

1. User with extension 201 calls number 5550199. *Kerio Operator* uses the rewriting rule which corresponds with the example in section 7.3 — firstly, *Kerio Operator* strips digit 2 from left which leaves number 01. The rule will append number 01. The final number is 0101.
2. Since the telephone provider requires only last four digits, the rule is complete and the number is sent to the telephone provider.
3. Telephone provider adds the rest of the number from left and the callee sees the calling number in format 5550101.

Make the following settings to ensure the above mentioned interface behavior:

1. In *Kerio Operator Administration* in section *Call Routing* doble-click on the interface in table *Routing of outgoing calls* (in our example, the interface with prefix 9).
2. This opens the *Edit Outbound Route* dialog and go to the *Rewrite Numbers* tab.

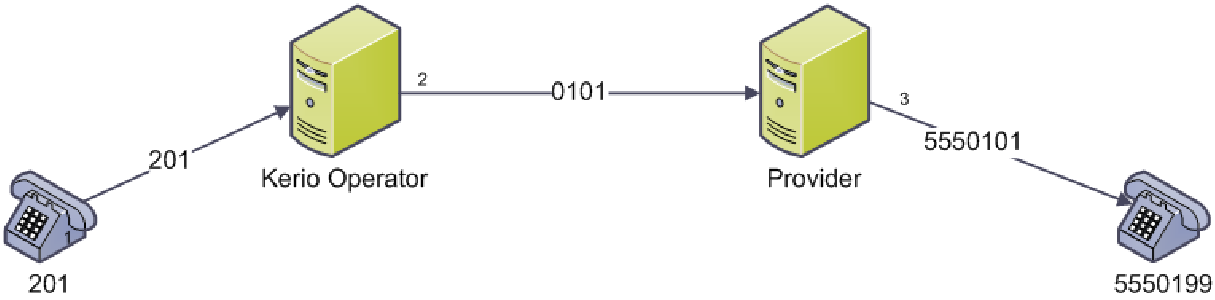
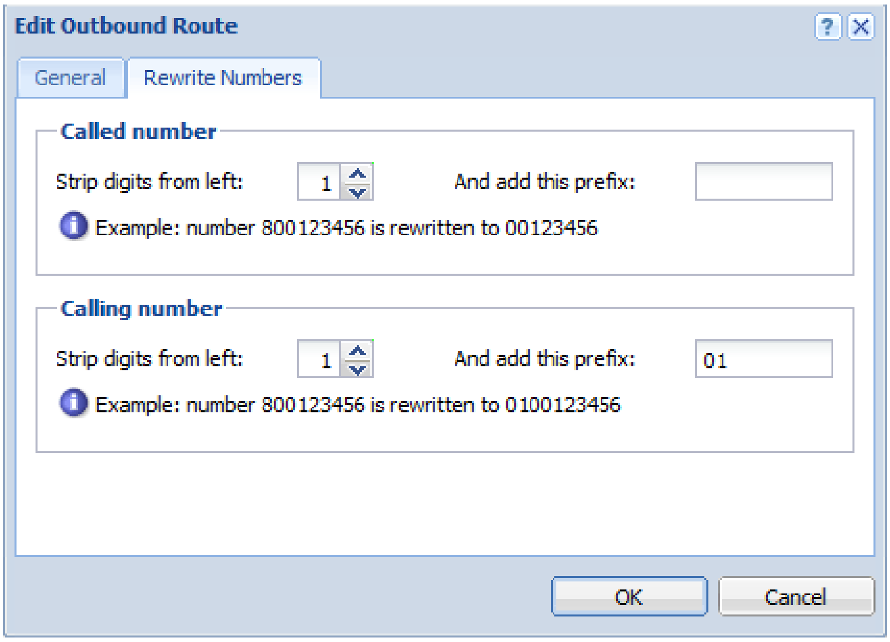


Figure 7.5 Scheme describing how to adapt calling number

3. We strip the prefix 9 from left in the called number (see figure 7.6).

4. We strip digit 2 from left in the calling number and add 01 (see figure 7.6).



Called number

Strip digits from left: 1 And add this prefix:

Example: number 800123456 is rewritten to 00123456

Calling number

Strip digits from left: 1 And add this prefix: 01

Example: number 800123456 is rewritten to 0100123456

Figure 7.6 Outbound Route

7.4 Overlap Dialing

Some telephone providrs require telephone numbers as a whole, others require the telephone numbers one digit at a time. Ask your provider about their requirements. Follow these steps to configure the interface:

1. In *Kerio Operator Administration*, go to section *Call Routing*.

2. Double-click the interface to open dialog *Configure PRI/BRI Interface*.

3. Switch to the *Interface card* tab.

4. If overlap dialing is required, check the *Overlap dialing* option.

Chapter 8

Configuring User Accounts and Phone Extensions

Kerio Operator has various configuration options. These options are available either for the whole PBX or for individual extensions. Extension configuration does not have to be maintained by the administrator. We recommend users to configure their extensions themselves. You can access *Kerio Operator* via two interfaces — *Kerio Operator Administration* and *Kerio MyPhone* (see chapter 3). The first interface is for system administrators and is used for general PBX configuration. The second interface is for users and is used for their extension(s) settings.

That is why *Kerio Operator* allows you to create and manage user accounts. The accounts are used:

- setting access rights for *Kerio Operator* (the *Kerio Operator Administration* or *Kerio MyPhone* interfaces),
- connecting an extension to a particular user (phone of Mr Smith is more convenient than phone with extension XY).
- setting PIN for voicemail connection,
- setting call forwarding to other number or numbers.

Accounts are:

- created locally,
- mapped from a directory service — *Active Directory* or *Apple Open Directory* (for more details on mapping, see chapter 11).

8.1 Creating Local Accounts and Assigning Extensions

New user account is defined in section *Users* by clicking the *Add* button:

1. In the edit dialog, enter username (diacritics, special symbols and space are not supported) and password.
2. Go to the *Extensions* tab and click on *Add*.
3. This opens the *Select Extension* dialog where all the *Kerio Operator* unassigned extensions are listed. Apart from these extensions, you can click on *Add* to open a dialog and create a new extension.

Note: First unassigned extension is prefilled in the *Extension number* field. If you do not wish to use this extension, delete it and enter a new extension.

4. Save the settings.

8.2 CallerID Settings

When calling to external network, users may wish to:

- display their own number — suitable for the majority of cases. The callees know who is calling them and may call back.
- hide their own number — suitable when we do not wish the callee to know our phone number (usually used in telemarketing). This function depends on the behavior of your provider.

  Note: If the extension number is hidden, it cannot log in to a call queue.
- exchange phone number for another one — enter another extension . For example, directors do not wish to display their number but the number of their assistant. If this is the case, enter the assistant's extension in the field.

All these settings are displayed when calling to an eternal network. When users make calls in the internal netwark of *Kerio Operator*, their real extension is displayed regardless of the above settings.

The caller's number is displayed by default. You can change the settings in section *Configuration → Users*:

1. Open the edit user dialog.
2. Go to the *Extensions* tab and double-click the extension you wish to edit.
3. Change the settings.

8.3 Call Routing Configuration

Incoming calls can be routed to different internal extensions or external numbers. The call may ring on all added telephone numbers at the same moment.

The next example shows the following settings: IT administrator in company XY requires calls to be redirected:

- his desk phone (internal extension in *Kerio Operator*),
- his company cell phone (to be available in case the server is down).

Configure the redirecting as follows:

1. Go to section *Users* and double-click the IT administrator account.
2. In edit user dialog, go to the *Ringing Rules* tab.
3. Here, the extension used by the administrator is checked. Click on *Add* and enter the cell phone number in an appropriate format (for example, 0602111111).
4. Save the settings.

Note: Users can also use the *Kerio MyPhone* interface to forward their calls.

8.4 Changing Access Rights

Kerio Operator uses the following system access roles:

- user — has righs to access the *Kerio MyPhone* interface.
- auditor — has rights to access the *Kerio MyPhone* interface and read only rights to *Kerio Operator Administration*
- administrator — has rights to access both the *Kerio MyPhone* and *Kerio Operator Administration* interfaces.

To change the user rights:

1. Go to section *Users*, select and double-click the user account.
2. In edit user dialog, go to the *Advanced* tab.
3. Change and save the settings.

8.5 Deactivating User Account

Each account in *Kerio Operator* can be deactivated by removing it permanently or disabling it temporarily.

Temporary deactivation

1. In section *Configuration* → *Users*, select the account you wish to deactivate.
2. Click on *Edit* or double-click the account.
3. This opens the *Edit user* dialog (see figure 9.1). Uncheck the *Account is enabled* option.

After saving the settings, the user will not be able to use their aacount until you enable it again.

Removing account

1. In section *Configuration* → *Users*, select the account you wish to disable.

2. Click on *Remove*.

Chapter 9

Phone Extensions

Phone extension is an internal phone number of *Kerio Operator*. Each extension is associated with particular settings and usually with a particular user who uses the extension. We recommend to created and assign extensions in section *Configuration* → *Users* (see chapter 8). Create extensions in section *Configuration* → *Extensions* only if you do not wish to assign them to particular users.

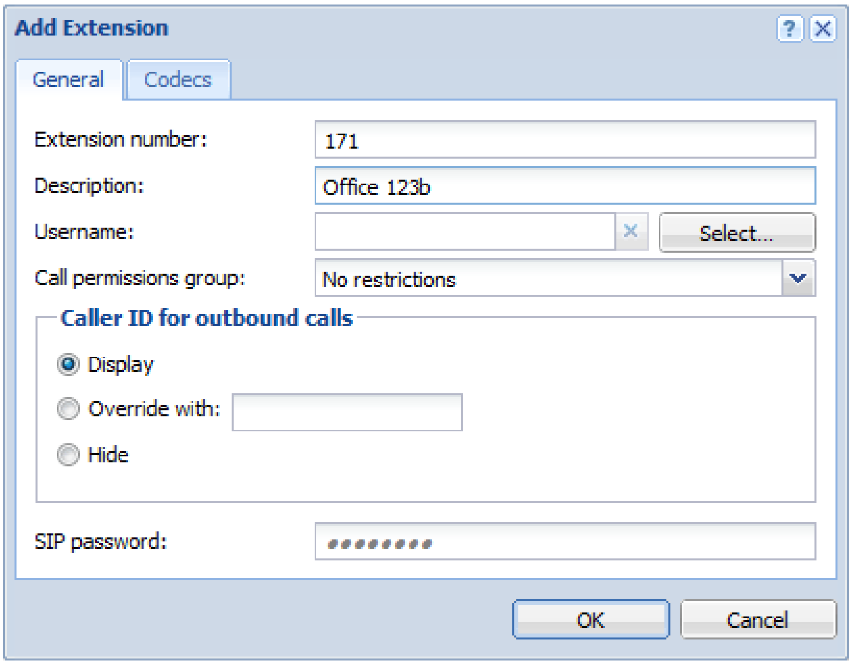
Phones are assigned extensions automatically or manually (for information about phone configuration, see chapter 10).

9.1 Creating a local extension

Creating extensions depends on the interfaces defining connections to an external network. The definition differs according to the number or numbers assigned by the VoIP service provider (for more information, see chapter 6). Make the definition in away to keep the internal extensions mapping as simple as possible.

To create a new extension:

1. In the *Extensions* section, click on *Add*.
2. In the *Add extension* dialog on the *General* tab, a new generated extension is displayed. You can change the extension number to meet your numbering plan policy.
3. (Optional) You can assign the extension to one of the users defined in the *Configuration* → *Users* section.
4. (Optional) You can limit outgoing calls for the extension (see section 23.2).
5. (Optional) You can decide whether the whole phone number will be displayed to the callee (see detailed description of this function in section 8.2).
6. (Optional) In the *SIP password* field, enter a password which will be used by the phone assigned to this extension to authenticate against *Kerio Operator* (set the same password in the phone).



Extension number: 171

Description: Office 123b

Username:

Call permissions group: No restrictions

Caller ID for outbound calls

● Display

○ Override with:

○ Hide

SIP password: ••••••••

Figure 9.1 Adding new extension

Chapter 10

Phone provisioning

Kerio Operator supports automatic phone provisioning of selected SIP phones thus simplifying the configuration of your phone network. Automatic phone provisioning means connecting the phone to a PBX, assigning it an extension and configuring other attributes. With automatic phone provisioning, a phone connects immediately after it boots in your local network for the first time.

Kerio Operator supports the following phones:

- Cisco 7940 and 7960 with the SIP firmware in version 3 and higher,
- Linksys SPA942, SPA962, SPA922, SPA901, PAP2T with firmware in version 5 and higher.
- Snom 300, 320, 360, 370, 820, 821, 870, M3 and Snom MeetingPoint.

Note: Kerio Technologies will make all efforts to broaden the list of supported phones. If you wish to connect a phone which is not currently supported in *Kerio Operator*, you cannot use automatic provisioning. The configuration must be done on the hardware phone.

We cannot employ automatic phone provisioning in the following situation: If you do not use the DHCP protocol in your network, automatic provisioning will not work.

Warning:
Automatic provisioning cannot always be used. If *Kerio Operator* is located and operated in the Internet, we do not recommend automatic phone provisioning for security reasons.

Phone provisioning requires:

- configuration of *Kerio Operator*,

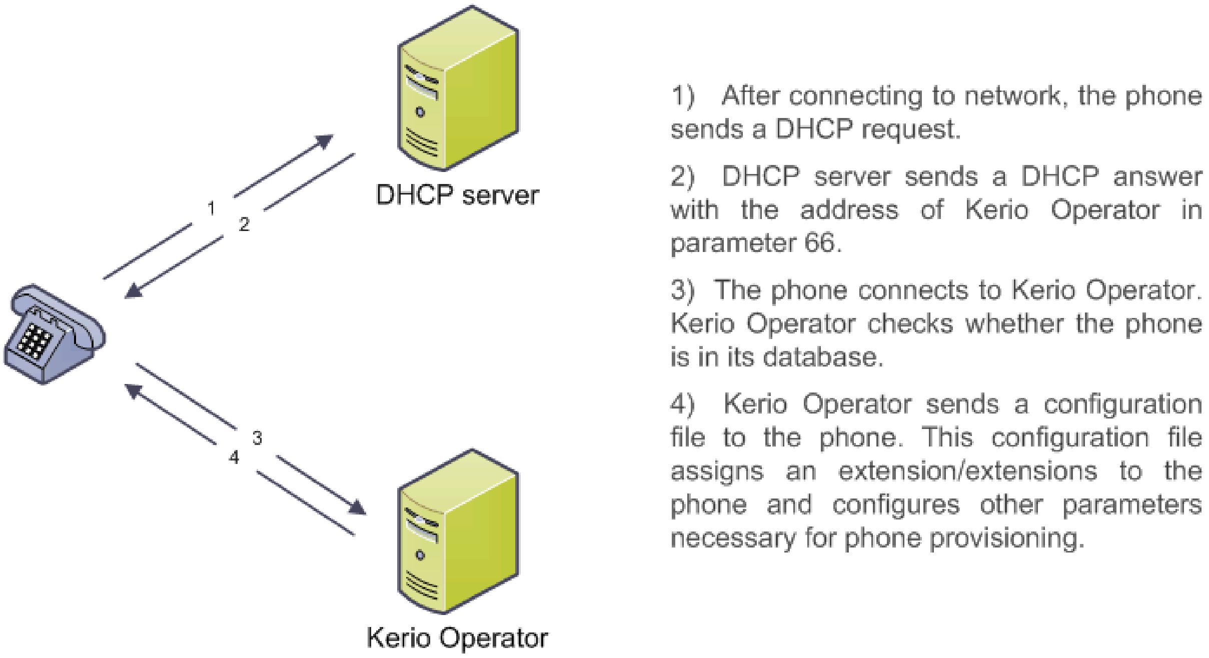
- running DHCP server supporting parameter 66 in your local network[1] (TFTP server address) — enter the address of *Kerio Operator*.

This is how the automatic provisioning works:

- The telephone boots in the network and sends a DHCP request for an IP address.

- DHCP server accepts the request, assign an IP address and sends it back in a DHCP reply. Apart from the IP address, the message also contains TFTP (Trivial File Transfer Protocol) server address — *Kerio Operator* in our case.

[1] DHCP server integrated in *Kerio Control* supports parameter 66.



1) After connecting to network, the phone sends a DHCP request.

2) DHCP server sends a DHCP answer with the address of Kerio Operator in parameter 66.

3) The phone connects to Kerio Operator. Kerio Operator checks whether the phone is in its database.

4) Kerio Operator sends a configuration file to the phone. This configuration file assigns an extension/extensions to the phone and configures other parameters necessary for phone provisioning.

Figure 10.1 Automatic HW phone provisioning

- SIP phone connects to TFTP server integrated in *Kerio Operator*.
- *Kerio Operator* checks whether the phone is new:
  - if it is new, *Kerio Operator* generates a new phone extension fro the phone;
  - if it is not new, *Kerio Operator* finds the extension which the phone has used.
- *Kerio Operator* generates a configuration file suitable for the particular phone type and sends it via the TFTP protocol.
- The phone is configured using the values it has acquired in the configuration file and is ready to be used.

10.1 Configuring the PBX

To configure automatic provisioning, go to section *Configuration → Provisioned Phones* in the *Kerio Operator* administration interface.

1. Check the *Enable provisioning* option.
2. In the *First extension* field, enter the extension number which will start the provisioning. If 10 is set, the first phone will be assigned extension 10, the next one 11, then 12, etc. If the extension is already used (e.g. if it has been created manually), it will be skipped.

   Select the first extension number according to your dial plan — for example, if you wish to have 3-digits extensions, star the numbering with 100.

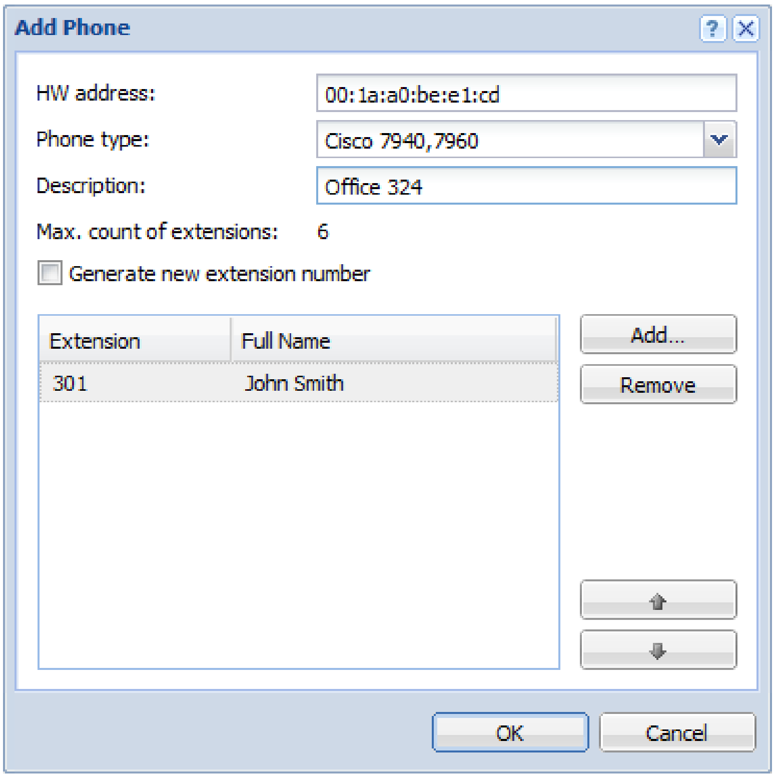
3. Decide whether to use option *Create new extension for newly registered phones*. Once this option is checked, *Kerio Operator* will assign the extension automatically. Otherwise, all new phones will be displayed in the *Provisioned Phones* table but will not be assigned any extensions. However, unchecking the option leaves you with better control over which extension is assigned to which phone.

4. The *Password for phones* field requires a strong password which all the automatically provisioned phones wil use to authenticate against *Kerio Operator*.[2]

Note: One phone can have assigned more extensions — it depends on the phone dispositions. You obtain the maximum number of extensions for each phone in its technical documention or during manual connection to *Kerio Operator* in the *Max. count of extensions* section (see figure 10.2).

10.2 Connecting phones manually

Phones which are not connected to the network can also be provisioned. We may do so manually — we need the phone's hardware address and the type of the phone (see figure 10.2). The procedure is described below:



Add Phone

HW address: 00:1a:a0:be:e1:cd

Phone type: Cisco 7940,7960

Description: Office 324

Max. count of extensions: 6

☐ Generate new extension number

Extension	Full Name
301	John Smith

Figure 10.2 Connecting a phone manually

[2] Each telephone must be authenticated when connecting to the PBX. Extension number and password are used for the authentication. If provisioning is used, this password will be applied for all provisioned phones. The password is saved in the configuration file which is sent to the phone upon the first connection to the network and on, the phone will use this password to authenticate at *Kerio Operator*.

1. In section *Configuration → Provisioned Phones*, click on the *Add manually* button.
2. This open a dialog which requires the hardware address of the phone (MAC address of the network card in the phone).
3. Select the correct type of the hardware phone (special configuration scripts are created according to the phone type).
4. Assign the phone user or users who will use it (see figure 10.2).

10.3 Importing from CSV file

Phones can be imported from a CSV file. Data in the file must follow certain rules:

- hwAddress — hardware address of the phone,
- phoneManufacturer — name of the phone's manufacturer,
- phoneType — phone type,
- extension1; extension2; ... — extensions assigned to the phone. The maximum number of extensions depends on the phone type.

Each phone uses one line and all items are devided by a semicolon.

The file may be as follows:

```
00:1a:a0:be:1e:cd;Cisco;794X;111;112
00:1b:b0:cd:e1:ca;Cisco;796X;115
00:1c:c0:ab:a2:24;Linksys;SPA942;113;114
```

Import data from a CSV file as described below:

1. In section *Configuration → Provisioned Phones*, click on the *Import from CSV* button.
2. This opens dialog *Import phones from CSV* and click on the *Upload CSV file* button.
3. If the data in the file are correct, a list of all the phones and extensions is displayed. Check those you want to import.
4. Confirm selection by clicking on *OK*.
5. The imported phones are displayed in the *Provisioned phones* table.

10.4 Removing a phone from Kerio Operator

If you wish to remove a phone from the telephone network, go to section *Configuration* → *Provisioned Phones*.

Select the phone you wih to remove and click on the *Remove* button.

You cannot remove a phone with any extensions assigned. Remove extensions as follows:

1. In section *Configuration* → *Provisioned Phones*, select the phone you wish to remove and click on *Edit*.
2. In the opened dialog, select the extension and click on the *Remove* button to remove it.
3. If more extensions are assigned to the phone, repeat step 2 for each extension. After removing the last extension click on *OK*.
4. Now, we can remove the phone in the *Configuration* → *Provisioned Phones* section by click the *Remove* button.

Note: Automatic phone provisioning option will be turned off for this phone, otherwise the phone would ask for configuration when connected to the network. If you want to use automatic phone provisioning again, we recommend to use so called “factory reset”.

10.5 Restarting provisioned phones

When you change phone provisioning configuration, all the phones need to be restared (for example, when you create new call route). When you do so, a dialog window recommending phone restart is displayed. You can do it immediately or wait for a more convenient time (for example to an off-peak time). The restart is described below:

1. Open the *Provisioned Phones* section.
2. Click on the *Advanced* → *Restart all phones* button.
3. This opens a dialog where you set the date and time for the restart if you wish to postpone it or click on the *OK* button.

10.6 Firmwares

Kerio Operator allows an easy installation of phone firmwares which are managed through the phone provisioning:

1. Go to section *Configuration* → *Provisioned Phones* and click on the *Advanced* → *Firmwares* button.
2. In the *Firmwares* dialog, click on *Upload*.

3. This opens a dialog where you select the firmware file and confirm the selection.

4. In the *New firware* dialog, select the appropriate phone.

5. Click *OK*. to confirm changes.

Chapter 11

Mapping Extensions / Users from Directory Services

Apart from locally created extensions (users accounts), *Kerio Operator* can also work with user accounts from *Active Directory* or *Apple Open Directory*. The benefits are as follows:

- user accounts can be managed from one location which reduces possible errors and simplifies administration,
- users can use the same username and password for login to their domain and to *Kerio MyPhone*.

Warning:

- Adding a new extension in *Kerio Operator* creates a local account — it will not be duplicated into the directory service database.
- When creating a user account in a directory service, ASCII must be used to specify username. If the username includes special characters or symbols, it might happen that the user cannot log in *Kerio MyPhone*.

11.1 Setting mapping in the administration interface

In the *Kerio Operator* administration interface, go to section *Configuration* → *Advanced Options* → *Directory Service*:

1. Check the *Map user accounts from a directory service* option and select the directory service type you use.
2. In the *Domain name* field, enter the name of your *Active Directory* or *Apple Open Directory* domain — the domain name is then duplicated in other necessary fields.

The dialog's form depends on whether you use *Active Directory* or *Apple Open Directory*.

Active Directory

1. In the *Hostname* field, enter the DNS name or IP address of the *Active Directory* server. If you have a backup server, enter its name in the *Secondary hostname (backup)* filed.
2. In the *Username* and *Password* fields, enter the authentication date of the user with at least read rights for *Active Directory* database. Username format is `user@domain`.
3. Within the communication of the *Active Directory* database with the PBX, sensitive data may be transmitted (such as user passwords). For this reason, it is recommended to secure such traffic by using SSL. To enable LDAPS in *Active Directory*, it is necessary to run a certification authority on the domain controller that is considered as trustworthy by *Kerio Operator*.
4. The rest of the items in the dialog are completed automatically. Do not change them unless you have a special reason to do so. These items are *Active Directory* domain name and Kerberos Realm which has to be the same as *Active Directory* domain name only written in capital letters.

Apple Open Directory

1. In the *Hostname* field, enter the DNS name or IP address of the *Apple Open Directory* server. If you have a backup server, enter its name in the *Secondary hostname* filed.
2. In the *Username* and *Password* fields, enter the authentication date of the user with at least read rights for the LDAP database. Username format is `user@domain`.

   This can be either user `root` or the *Open Directory* administrator (`diradmin`). In case that the administrator's username is used, it is necessary to make sure the user is an *OpenDirectory* Administrator, not just a local administrator on the *OpenDirectory* computer.

   To connect to the *Apple OpenDirectory* database insert an appropriate username in the following form:

   `uid=xxx,cn=xxx,dc=xxx`

   - `uid` — username that you use to connect to the system.
   - `cn` — name of the users container (typically the `users` file).
   - `dc` — names of the domain and of all its subdomains (i.e. `company.com` → `dc=company,dc=com`)
3. Within the communication of the LDAP database with the PBX, sensitive data may be transmitted (such as user passwords). It is possible to secure the communication by using an SSL tunnel.
4. The rest of the items in the dialog are completed automatically. Do not change them unless you have a special reason to do so. These items are *LDAP search suffix* (usually

`dc=subdomain,dc=domain`) and Kerberos Realm which has to be the same as *Apple Open Directory* domain name only written in capital letters.

Chapter 12

Dial Plan

The dial plan contain a list of all the used extensions and their users. You can export this list to a CSV file or print it.

Go to section *Configuration* → *Dial Plan* to see the list:

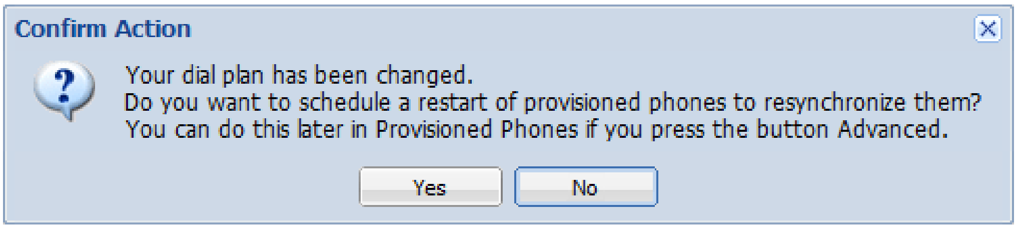
Export to CSV — the button exports the data in the format discribed in table 12.1.

Extension Number	Type ID	Description
111	1	Winston Smith
112	1	Ada Monroe
50	7	Voicemail

Table 12.1 CSV file content

12.1 Changing the Dial Plan

If you use automatic phone provisioning and the change in your dial plan may affect automatically provisioned phones, update of the phones configuration is needed. *Kerio Operator* detects such changes automatically and displays a warning (see figure 12.1). If you confirm it, the phones are immedeately remotely restarted. You can restart the phones later manually in section *Provisioned Phones*. To restart the phones, click on the *Advanced* → *Restart all phones* button.



Confirm Action

Your dial plan has been changed.
Do you want to schedule a restart of provisioned phones to resynchronize them?
You can do this later in Provisioned Phones if you press the button Advanced.

Figure 12.1 Changing the Dial Plan

Chapter 13

Telephone Conferences

Telephone conferences are calls with more than two participants (i.e. phone numbers / extension).

Telephone conferences allow participation both of users defined in *Kerio Operator* and external participants. To join the particular conference it is only necessary to enter conference number and possibly also its access code.

13.1 Creating New Conference

1. Go to section *Configuration* → *Extensions* and make sure that the line you have selected for the conference is not used.
2. Add new conference in section *Configuration* → *Conferences*.
3. Click on *Add*. This open the *Add conference* dialog.
4. Enter the conference extension and its description.
5. Optinally, you can limit the number of participants. Too many participants an increase demands on the server and affect its performance
6. Each conference can be protected by a PIN required at the entrance from all participants. If you wish to secure your conference (especially if the conference will hold strategic meetings and negotiations), set the PIN and distribute it among all the participants.

13.2 Conference login / logout

To join a conference, follow these steps:

1. Dial the conference telephone number / extension.
2. If the conference is protected, you will be asked to enter the PIN.

To leave the conference, simply close the call.

13.3 Viewing Active Conferences

All current conferences can be viewed under *Status* → *Conferences*. This section displayed a table where each conference occupies one line.

Aart from the conferences, you can also see detailed information about individual participants. Select the conference and click on the *Show Details* button. The displayed dialog shows the number of current members of the conference and time since their login.

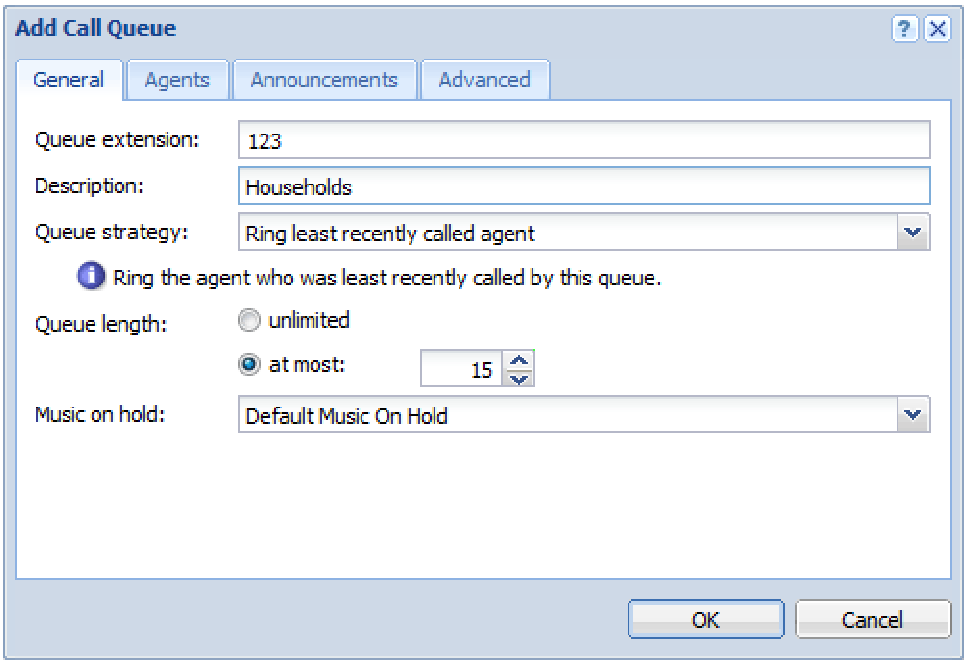
Chapter 14

Call Queues

Call queue is a tool which enables your customers to be placed in a queue and gradually assigned to your employees.

14.1 Defining Call Queue

Create a new call queue in section *Configuration* → *Call Queues* by clicking on *Add*.



Queue extension: 123

Description: Households

Queue strategy: Ring least recently called agent

Ring the agent who was least recently called by this queue.

Queue length: ○ unlimited ● at most: 15

Music on hold: Default Music On Hold

Figure 14.1 Call Queue — General tab

1. On the *General* tab (see figure 14.1), fill in such exntension that is not used (see section *Configuration* → *Dial Plan*).

2. Enter *Description* which will later define the queue in the queue list.

3. Now choose a queue strategy:

    - Round robin with memory — agents (for more information on agents, see section 14.2) are called repeatedly in the same order.

    - Ring all agents — calls are always ringing at all agents until one of them answers the particular call.

- Ring least recently called agent — the system selects the agents who has not answered the phone for the longest period.
- Ring agent with fewest calls — the system assigns the call to the agent with the lowest number of calls answered so far.
- Ring random agent — if you select this option, the system will choose an agent randomly.

4. Now change the length of the call queue. The length of the call queue represents the maximum number of queued callers. It can be set to *unlimited* or you can limit it to a specific number. Maximum number of calls in a queue is 999.

   We recommend to set this limit when you know how many people call the number and what is their waiting time. If callers wait too long, we advise to set a limit. Long waiting in a queue may discourage customers even more than not having been queued at all.

5. Eventually, you can configure the queue's music on hold. If you want to use your own, you have to add to *Kerio Operator* (see chapter 24).

14.2 Agents

Agents are telephone operators who attend the call queue and answer customer demands. The caller calls the queue number, waits for the connection and then is connected to the agent who will handle their demands (see figure 14.2).

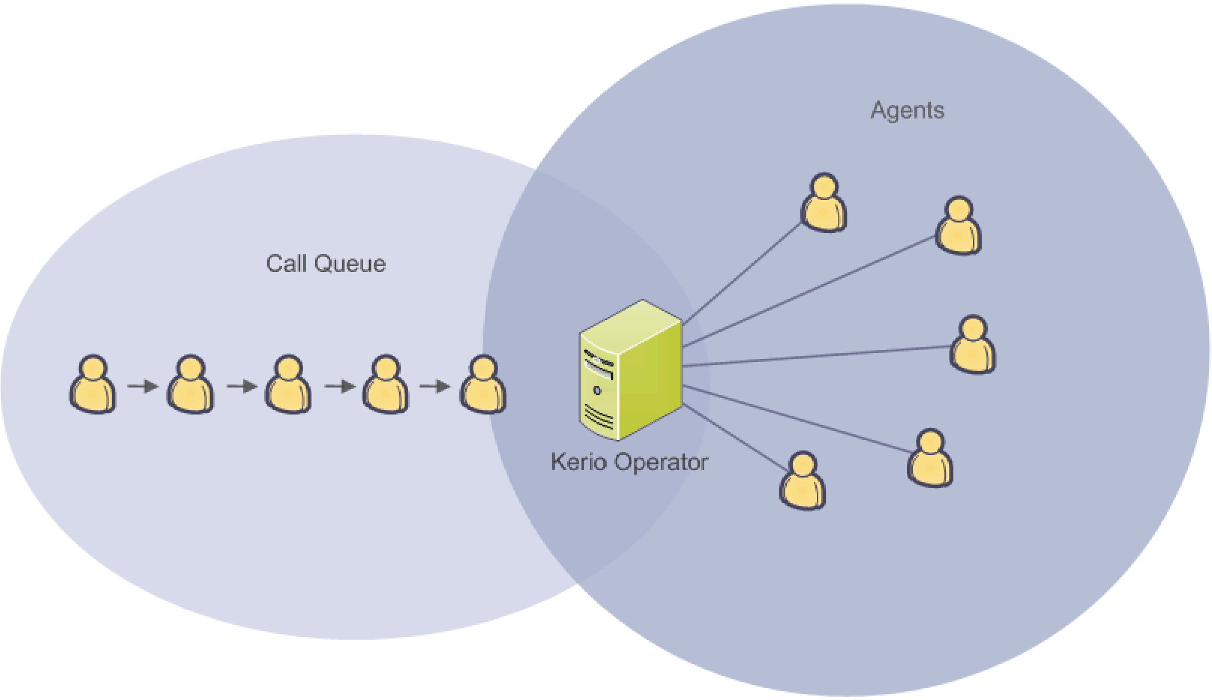


Figure 14.2 Call queue

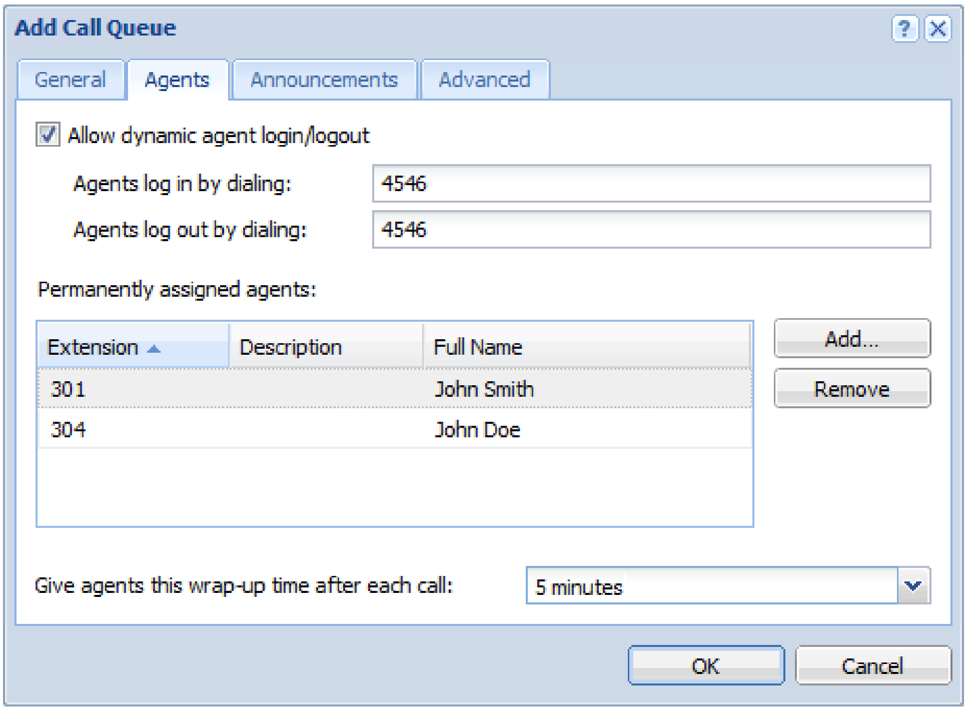
Call Queue login / logout

Callers login to the queue by calling the queue's number. Agents can login wither dynamically by dialing a special number or their extension can be permanentally assigned to the queue. The settings depends upon your company's policy.

- Dynamic login/logout — each agent has their own phone and table. After arriving to work, they login to the queue using a special code and later they logout.
- Permanent login — agents take turns operating phones in shifts (non-stop call centers) — the phone is permanently assigned to a queue and agents take turns operating one phone.
- Combination of both the above options. Some agents are permanently assigned and others login dynamically. This is convenient during the peek-hour shift. The queue is then attended by more agents than in other shifts.

Apply settings as described below:

1. Select the call queue or create a new one (section 14.1) in section *Configuration* → *Call Queues*.
2. GIn the displayed dialog, go to tab *Agents* (see figure 14.3):



☑ Allow dynamic agent login/logout

Agents log in by dialing: 4546

Agents log out by dialing: 4546

Permanently assigned agents:

Extension ▲	Description	Full Name
301		John Smith
304		John Doe

Give agents this wrap-up time after each call: 5 minutes

Figure 14.3 Call Queue — Agents tab

Dynamic login
Check the *Allow dynamic agent login/logout* and eneter codes for the queues login and logout. Make sure the codes are different from the extension numbers.

Permanent login
Click on *Add* and enter the agent's extension.

3. Regardless of the queue strategy, you may set time when no call will be connected to the agent. This enables the agnt to process the call. If your agents need to fill in a rcord after each call, set the appropriate in the *Give agents this wrap-up time after each call* menu.

Operating more queues at once

Agents do not ahve to operate one queue at a time (see figure 14.4). Our example illustrates the queue use in a fictional electricity provider. This company has one queue for households, one for businesses and another one for VIP customers. Since questions about electricity outages and due invoices are similar with different services available to different customers, the queues are operated by the same agents.

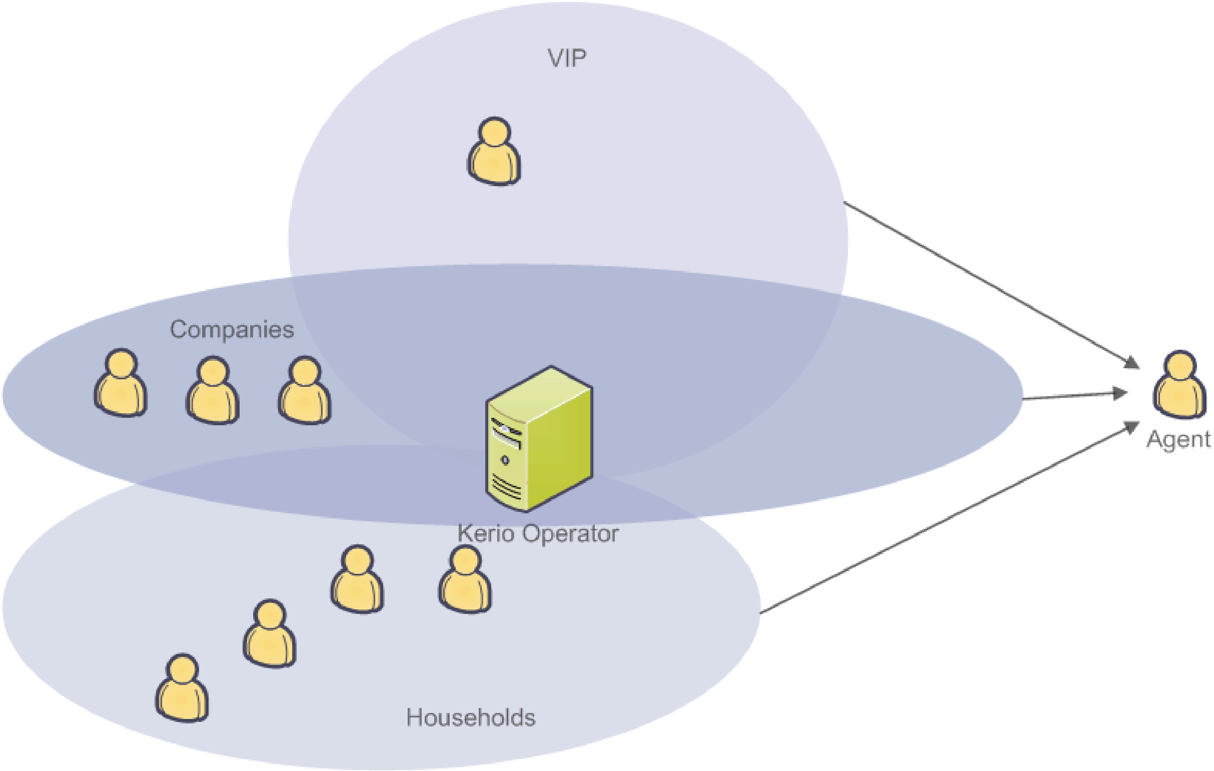


Figure 14.4 Operating more queues at once

To help agents identify the queues, you can upload various recordings for each queues. The recording identifying a queue is played to the agents before a call from this queues is connected.

Upload new recoding as follows:

1. Select the call queue or create a new one (section 14.1) in section *Configuration → Call Queues*.

2. In the displayed dialog, go to tab *Announcements*.

3. Check the*Help agents identify the source queue by playing this announcement* and click on *Select*.

4. This opens the *Select Audio File* dialog. You can either double-click a recording to select it or upload your own recording to *Kerio Operator* (it must be in WAV or GSM format). Use the *Upload* button.

   You can play a recording by selecting it and clicking on *Play*.

It is also possible to set priorities for individual queues. Queues with higher priority will be process earlier. In our example (see figure 14.4), the electricity provider may use the following priorities:

- VIP — high priority,
- Businesses — medium priority,
- Households — low priority.

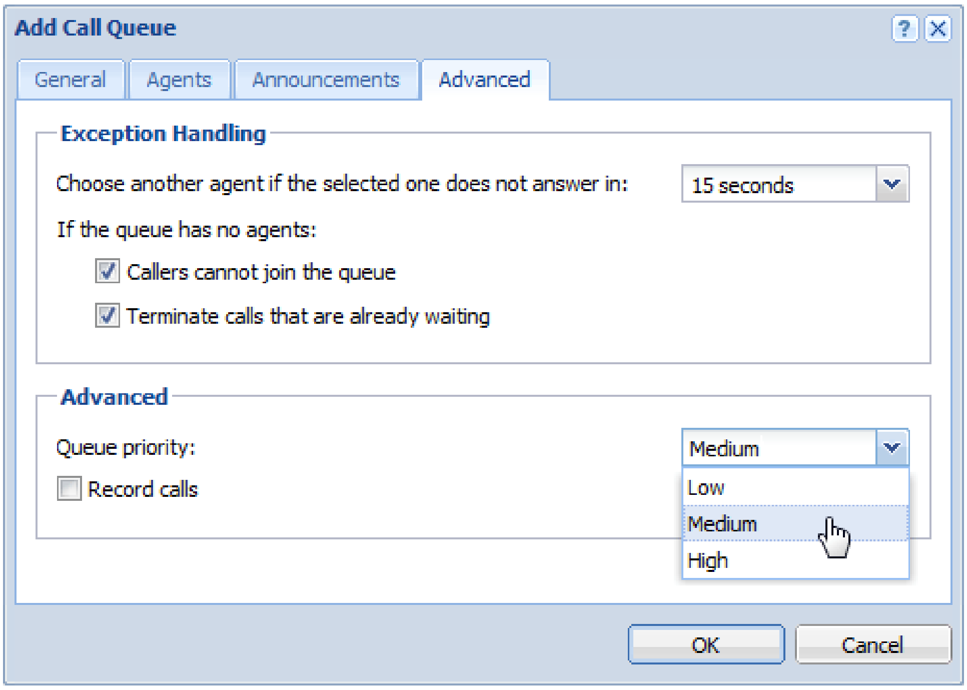
Apply settings as described below:

1. Open the *Configuration → Call Queues* section.

2. Select a queue or create a new one (section 14.1).

3. In the displayed dialog, go to tab *Advanced* and set the desired priority (see figure 14.5):

4. Repeat the configuration for other queues.



Add Call Queue

General | Agents | Announcements | Advanced

Exception Handling

Choose another agent if the selected one does not answer in: 15 seconds

If the queue has no agents:

☑ Callers cannot join the queue

☑ Terminate calls that are already waiting

Advanced

Queue priority: Medium

□ Record calls

Figure 14.5 Call Queue — Advanced tab

Agent Does Not Answer

The following situations may occur during call queues operation:

- Agents does not answer the phone even though they are connected to the queue.
- In case all agents use dynamic login, the queue may not have any agents available.

Go to section *Configuration* → *Call Queues* to configure *Kerio Operator*:

1. Select the call queue:
2. In the displayed dialog, go to tab *Advanced* (see figure 14.5).
3. In the *Exception Handling* section, set the time limit for actions when agent does not answer the call. When the time limit expires, the call will be directed to the next agent according to the queue strategy.
4. If no agents is currently assigned to the queue, it is possible to prevent new callers from being queued. Also, you can check the option that all already waiting calls would be disconnected. Check both option especially when the call center working hours are limited. For example, if your call center works from `8am` to `5pm` and there are three customers in the queue after 5pm when all agents have logged out, they could theoretically wait till morning for agents to login and handle their call.

14.3 Announcements for Callers in a Queue

Customer waiting in a call queue can receive the following informationwhile waiting:

- customer's position in the queue
- estimated hold time (*Kerio Operator* is able to count the average waiting time of the previous customers),
- another announcement (for example promotinal announcement or an apology for waiting) which can be periodically repeated.

You can also set the language of these announcements.

Apply these settings by using the following instructions:

1. Open the *Configuration* → *Call Queues* section and select the queue.
2. In the displayed dialog, go to tab *Announcements*.
3. In the *Customers* section, click on *Select* to set the periodic announcement.
4. This opens the *Select Audio File* dialog. Double-click a file to upload it to the system.
5. If the file is not available, click the *Upload* button to upload it to *Kerio Operator* from your computer.
6. Set the repeat cycle.
7. Select the repeat cycle for the position in queue announcement.
8. If you wish your customer to know the estimated waiting time in the queue, check the *Include estimated hold time*.
9. Eventually, you can select the announcement language.

14.4 Recording Calls

Kerio Operator allows recording calls from call queues. No other module or equipment is necessary. Setting can be done as follows:

1. Open the *Configuration* → *Call Queues* section and select the queue in which you wish to record the calls.
2. In the displayed dialog, go to tab *Advanced*.
3. Check the *Record calls* option.

List of recorded calls

All recorded calls from call queues are also listed in a special table. They can be found in section *Status* → *Recorded Calls*. This section displayed a table where each recorded call occupies one line.

Deleting Recorded Calls

Recorded calls can be periodically deleted once their total size reaches a certain limit. The limit can be set in section *Status* → *Recorded Calls*.

1. Click on button *Advanced* → *Periodically Remove Old Recorded Calls*.

2. This open dialog *Remove Old Recorded Calls* where you enter the maximum size of recorded calls on a disk (in MB). Once the limit is reached, the oldest calls is deleted.

14.5 Viewing Call Queues

All active call queues and their parameters can be observed in section *Status* → *Call queues*. This section displayed atable where each call queue occupies one line.

Apart from all created call queues, it includes detailed information about individual queue agents. Select the queue and click on the *Show Agents* button. This display a dialog with information about the number of agents in the queue, how many calls they have handled and so on.

It is also possible to view detailed information about callers. Select the queue and click on the *Show Callers* button. You learn the callers' telephone numbers, their position in the queue or their waiting time.

You can slo reset the call queue statistics to start from zero. Use the *Reser Statistics* button.

Chapter 15

Ringing Groups

This chapter describes the *Ringing Groups* function which allows ringing on several phone extensions. For example, various Sales Department emplyees can answer callers' questions. The call rings on multiple phones at a time. This allows any salesman on the specific numbers to answer the call.

15.1 Creating Ringing Group

To create a new ringing group, go to *Ringing Groups* and click on *Add*:

1. Enter the extension number in the *Group extension* field.

2. In the table, add extensions of all users who will belong to the group.

3. If you wish to direct the call to another person when noone from the ringing group answers the phone, check the *Fall back to another extension when the group is not responding*

Chapter 16

Auto Attendant Scripts

Section *Auto Attendant Scripts* contains scripts for voice menus. These menus play voice announcements to incoming calls. Auto attendant scripts will help your company improve your customer care and lower its costs. Customers receives information directly or they will be connected, as soon as possible, to an extension with agent ready to help him. Auto attendat script offers the caller various options in recorded menus and by pressing different buttons the caller will be connected to an extension.

Auto Attendant Scripts allows:

- Quickly connect the caller to desired extension, to desired department — *Kerio Operator* handle more calls.
- Answer frequently asked questions — customers get necessay information (for example, address or opening hours) withou waiting.
- Raise the productivity of your employees — it reduces the time your employees spend connecting calls.
- Availability to callers out of office hours.
- Select the language for communication — if the auto attendant script has menus in different languages available, the callers can select in which language they wish to communicate.

Auto attendant script is a simple collection of voice menus, submenus and announcements and actions defined for each of them according to the caller's behaviour. It can:

- connect to an extension or voicemail,
- play an announcement,
- navigate through menus and submenu and repeat them.

Menus can be recorded in various formats. *Kerio Operator* supports the following formats (see table 16.1):

Supported formats	Audio format
gsm	8KHz
wav	8KHz, 16 bits per sample , mono (*Kerio Operator* encodes all WAV files into this format automatically)

Table 16.1 Kerio Operator — supported audio formats

16.1 Add Auto Attendant Script

See the following description of an auto attendant script as an example: Create a script which:

- starts after dialing extension 200,
- contain a voice menu woth the foloowing text: Hello, you have reached the customer support of Company Ltd.
    - For Sales Department, press 1.
    - For Purchasing Department, press 2.
    - For Technical Support Department, press 3.
    - If you wish to speak to the receptionist, press 4.

The Sales Department manages two products of the company. Therefore, two submenus (product 1, product 2) are created.

- For Product1, press 1.
- For Product2, press 2.
- If you wish to speak to the receptionist, press 3.

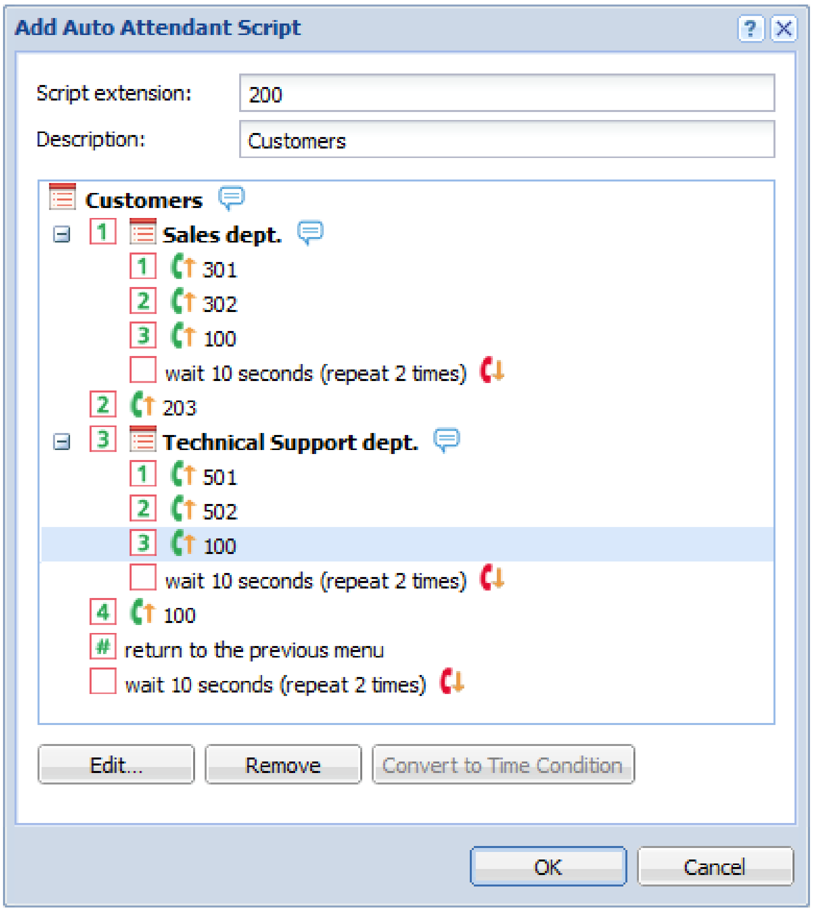
Create the same menu for technical support.

Before creating the script, it is necessary to create extensions (in the assigned range 123456XXX) which will be used in the script.

- *extension 100* — reception of *Company.cz*. The receptionist will conect the calls if the caller makes no selection from the menu.
- *extension 203* — Purchasing Department extension.
- *extension 301* — common extension for employees with Product1 (we can create a call queue or a ringing group).
- *extension 302* — common extension for employees with Product2.
- *extension 501* — call queue for Technical Support of Product1.
- *extension 502* — call queue for Technical Support of Product2

Script settings

Configure the script in the administration interface in section *Configuration* → *Auto Attendant Scripts*:



Script extension: 200

Description: Customers

- **Customers**
  - 1 **Sales dept.**
    - 1 301
    - 2 302
    - 3 100
    - wait 10 seconds (repeat 2 times)
  - 2 203
  - 3 **Technical Support dept.**
    - 1 501
    - 2 502
    - 3 100
    - wait 10 seconds (repeat 2 times)
  - 4 100
  - # return to the previous menu
  - wait 10 seconds (repeat 2 times)

Figure 16.1 Auto Attendant Scripts

1. Click on *Add* and enter the *Script extension* (extension 200 in our example) and some description (see figure 16.1).

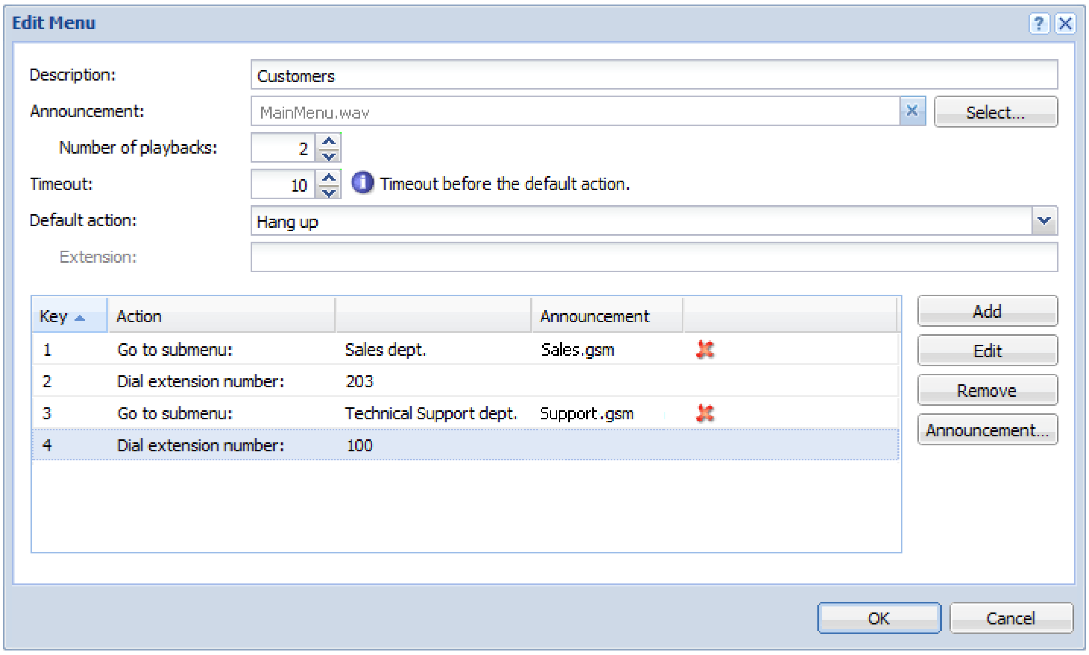
2. Click on the *Edit* button and open the *Edit Menu* dialog.

3. Select an anouncement for the main menu in the *Announcement* field. The *Select* button offers existing recordings or we can upload our own announcement from the computer.

4. Set the number of playbacks to two which will ensure the menu is played to the caller two times.

5. Once the announcement is played, timeout is started with the default action taken upon its expiration. Set the timeout to 10 seconds. The default action is the preset hang up. This means that if the announcement is played twice and the customer will not amke any selection within 10 seconds, the call will be terminated so that the extension is not blocked.

6. Click on the *Add* button to add a new line to the table. The *Key* column states the key which confirms the customer's choice. Enter 1 in this column. Column *Action* defines what happens when the caller presses a key on their phone. Select option *Go to submenu* to direct calling customers to the extension of the product they are interested in. In the *Announcement* column, you can add a record which will be played upon pressing the particular key (for example, Now you will be redirected to the Sales Department). Finish the table according to figure 16.1.



Description: Customers

Announcement: MainMenu.wav

Number of playbacks: 2

Timeout: 10 Timeout before the default action.

Default action: Hang up

Extension:

Key	Action		Announcement	
1	Go to submenu:	Sales dept.	Sales.gsm	✗
2	Dial extension number:	203		
3	Go to submenu:	Technical Support dept.	Support.gsm	✗
4	Dial extension number:	100		

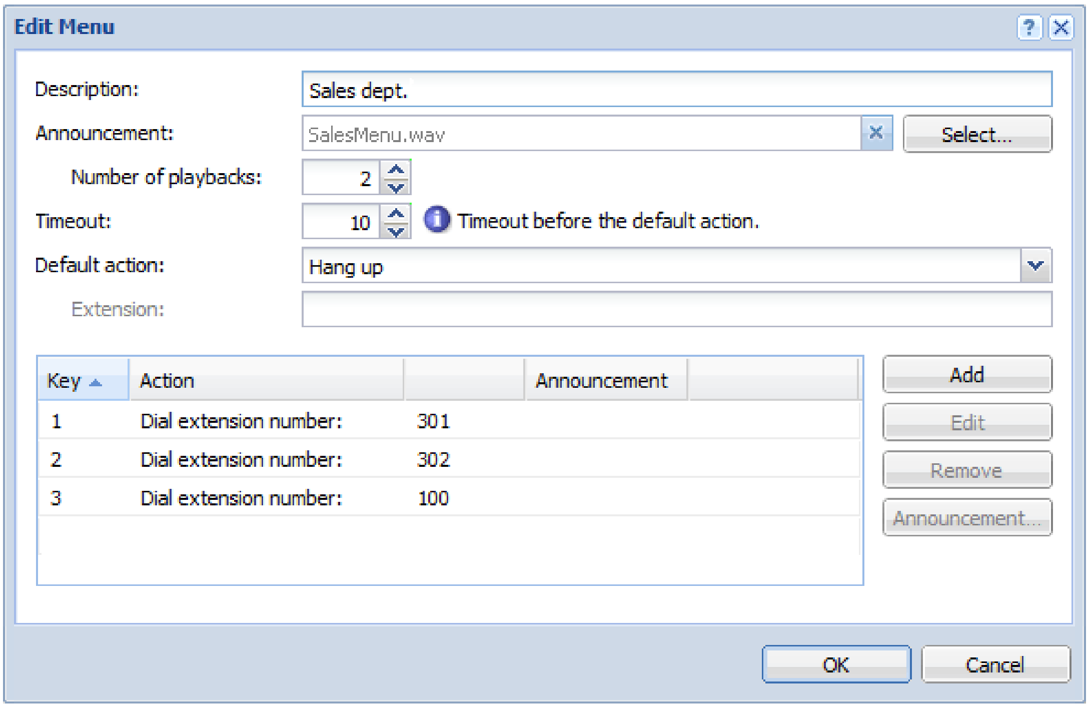
Figure 16.2 Editing main menu

7. Confirm the settings and return to the *Add Auto Attendant Script* dialog which is now similar to the one in figure 16.1.

8. Click on the *Sales Dept.* menu. Again, the Edit menu dialog is opened but now the menu is for the Sales department. Proceed similarly as with the main menu. The final menu will look as the one in figure 16.3.

9. Do the same for the *Technical Support dept.* menu.

10. Now the script from our example is complete.



Edit Menu

Description: Sales dept.

Announcement: SalesMenu.wav

Number of playbacks: 2

Timeout: 10 Timeout before the default action.

Default action: Hang up

Extension:

Key	Action		Announcement
1	Dial extension number:	301	
2	Dial extension number:	302	
3	Dial extension number:	100	

Figure 16.3 Submenu edit

Time condition

The script can be limited to a specific time interval (office hours of your employees or night time when no call queue agents are available).

The time ranges (intervals) are configured in section *Configuration* → *Definitions* → *Time Ranges* (see section 25). Once you have the time range configured, go back to the *Add Auto Attendant Script*, select the menu you wish to limit and click on the *Convert to Time Condition* button.

The following example describes use of time condition in context of working hours. Sales department works from 9am to 5pm on weekdays. we must configure the auto attendant script so that when customers call during office hours they will be connected to a sales department employee and when they call before or later they will hear a message announcing that the sales department is closed. To create the condition script, follow these instructions:

1. In the administration interface, go to *Configuration* → *Definitions* → *Time Ranges*.
2. Click on *Add*.
3. This open dialog *Add Time Range*. In section *Add to a group*, select the *Create new* option and enter a name for the new interval (for example, `Sales Department Office Hours`).
4. The *Description* is optional, for example *Weekdays from 9am to 5pm*.
5. Select `daily` in the *Type* menu and set the desired interval from 9 to 5 in the *From* and *To* fields.

6. In the *Valid on* menu, select *Weekdays*.

7. Click *OK*. to confirm changes.

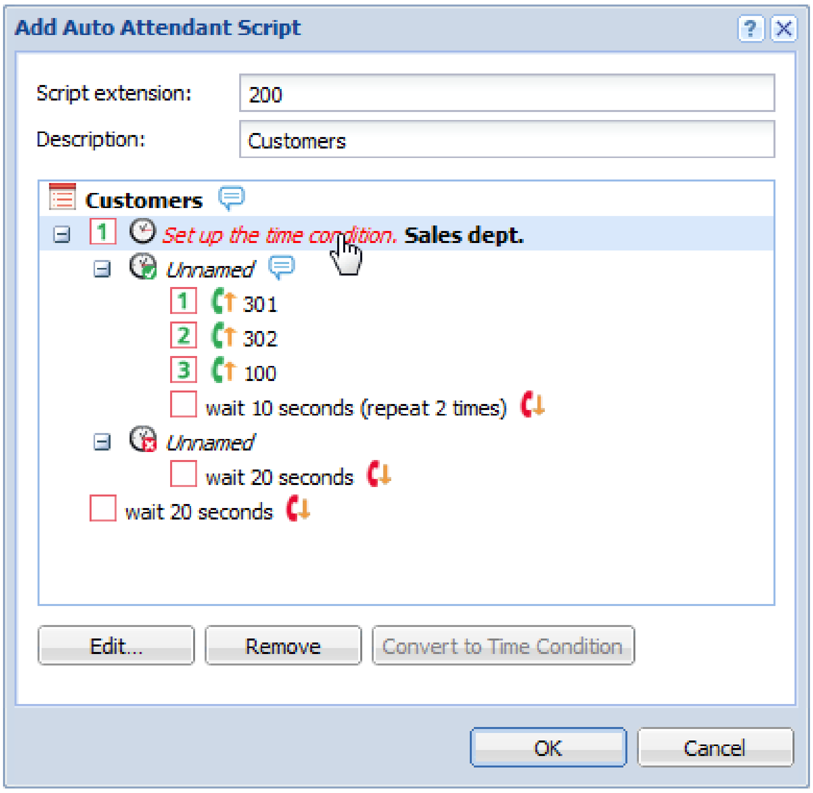
8. Open the *Configuration* → *Auto Attendat Scripts* section.

9. Click on *Add*.

10. In the *Add Auto Attendant Script* dialog, create a corresponding menu (the script created in the previous section will be used in this example — see figure 16.1).

11. Select the *Sales Department* submenu and click on *Convert to Time Condition*.

12. Divide the Sales Department submenu in two time conditions. The first plays if the condition is met and the second if the condition is not met. Click on the red highlighted text *Set up the time condition* (see figure 16.4).



Add Auto Attendant Script

Script extension: 200

Description: Customers

```
Customers
⊟ 1 Set up the time condition. Sales dept.
    ⊟ Unnamed
        1 301
        2 302
        3 100
        □ wait 10 seconds (repeat 2 times)
    ⊟ Unnamed
        □ wait 20 seconds
  □ wait 20 seconds
```

Figure 16.4 Setting the time condition

13. This opens dialog *Edit Time Condition*. In the *For time range* menu, select *Sales Department Office Hours*.

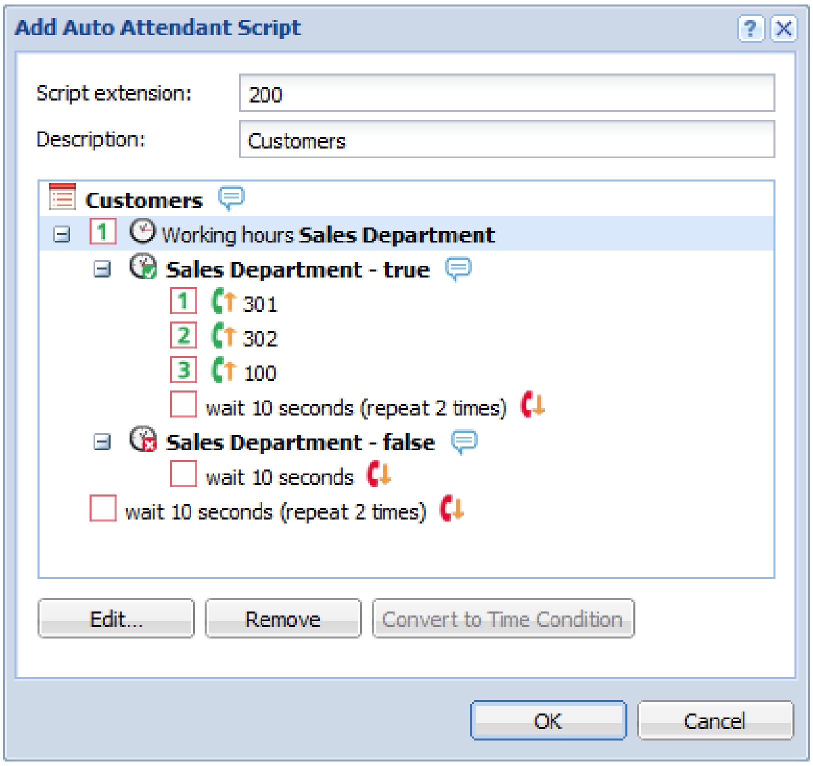
14. Click on the submenu representing the positive part of the condition. It is currently called *Unnamed*. In the dialog *Edit Menu* just opened, simply add a description (for example `Sales Department --- condition met`).

15. Click on the submenu representing the negative part of the condition (now it is empty and unnamed).

16. This opens dialog *Edit Time Condition* allowing to add a description (for example `Sales Department --- condition not met`).

17. Now modify the script. For example, in the *Announcement* field, add a message announcing that office hours of the Sales Department are from 9am to 5pm on weekdays.

18. Save the submenu. The final script is in figure 16.5.



Script extension: 200

Description: Customers

```
Customers
⊟ 1 Working hours Sales Department
    ⊟ Sales Department - true
        1 301
        2 302
        3 100
        □ wait 10 seconds (repeat 2 times)
    ⊟ Sales Department - false
        □ wait 10 seconds
    □ wait 10 seconds (repeat 2 times)
```

Figure 16.5 Time condition applied in the script

Chapter 17

Voicemail

Voicemail allows callers leave a voice message for the called person. It works similarly as a hardware message recorder but messages are stored on the server and they can be forwarded to user email boxes.

If you use both *Kerio Operator* and *Kerio Connect*, you can benefit from their cooperation and possible synchronization of voicemail messages.

Voicemail allows:

- forwarding to voicemail if the user is unavailable,
- forwarding to voicemail if the user is busy,
- direct access to user voicemail,
- sending voice messages to your email box.

17.1 Voicemail Settings

To launch and configue the voicemail in *Kerio Operator*, go to section *Configuration* → *Voicemail*:

1. Check the *Redirect the call to voicemail if the user is unavailable* option. From now on, the voicemail is available to all users.
2. According to the users' need, you can also set forwarding to voicemail when the callee is busy.
3. In the *Voicemail access extension* field, enter an extension number — once the users dial this extension and enter thier PIN number, they are connected to their voicemail and can play their voicemail messages.
4. Set each user their PIN on the *General* tab in section *Configuration* → *Users* (see section 9.1).

17.2 Direct access to user voicemail

Direct access to users' voicemail enables the receptionist to connect calls directly to callee's voicemail.

To configue the direct access to voicemail in *Kerio Operator*, go to section *Configuration* → *Voicemail*:

1. Check the *Allow direct dialing to user's voicemail boxes* option.

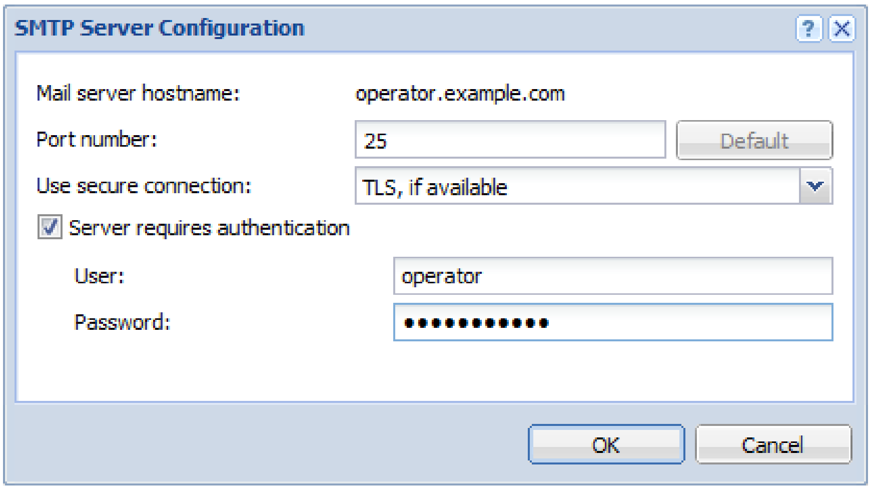
2. Enter an extension in the *Prefix for direct dialing* field.

Save the settings. Now the receptionist can dial the extension for direct access followed by the user's extension. The caller will be directed to the voicemail of the person they are calling.

17.3 Sending Voicemail Messages to User's Mailbox

Users welcome the possibility to forward their voicemail messages to their email box. Emails are sent via the standard SMTP protocol (Simple Mail Transfer Protocol), port 25.

To configure sending of voicemail message to users' mailboxes, go to section *Configuration* → *Voicemail*:



SMTP Server Configuration

Mail server hostname: operator.example.com

Port number: 25

Use secure connection: TLS, if available

☑ Server requires authentication

User: operator

Password: ●●●●●●●●●●●

Figure 17.1 SMTP configuration for sending voicemail messages

1. On your mail server, create a special user which will be used for sending the voicemail messages. You can name them for example `operator`.

2. Go to *Kerio Operator Administration* to section *Configuration* → *Voicemail* and check the *Send each mesage to user's email* option.

3. In the *Mail server hostname* field, enter the IP address or name of your SMTP server and click on *SMTP Configuration*.

4. Set the port number to the port used by your SMTP server (usually 25 for SMTP and 465 for SMTPS).

5. Decide whether to communicate through secured connection. You can choose unencrypted connection, SSL encryption or TLS encryption. If the configuration of your mail server allows it, we recommend the encrypted connection to establish more secure communication.

6. If your SMT server requires authentication, check the *Server requires authentication*. Use the username and password for the account you created on your mail server in step 1 (see figure 17.1).

7. Click OK to confirm settings.

8. In *Configuration* → *Voicemail* in the *Sender email address* field, enter the email address of the user you created in step 1.

To send voicemail message to email boxes of the users, you need to set their email address in the *Kerio Operator Administration* in section *Configuration* → *Users*. For more information refer to section 17.4.

Integrate with Kerio Connect

Integration with *Kerio Connect* allows synchronization of the flag marking whether the message has already been read/played. This means that if you mark a message as read in *Kerio MyPhone* or if the message is marked as read after you hear it on your phone, the message will also be flagged as read in your mail box (and vice versa).

If integration with *Kerio Connect* is set, voicemail messages are not stored in *Kerio Operator* but in user's *Inbox* on the mail server.

To configure the integratation, follow these instructions:

1. Go to *Kerio Operator Administration* to section *Configuration* → *Voicemail* and switch the SMTP server settings to *Integrate with Kerio Connect*.

2. Click on *Configure*, enter the DNS name or IP address where *Kerio Connect* is running and specify name and password of a user with admin rights to the *Kerio Connect* server.[3]

   Note: To synchronize flags between the two servers, *Kerio Operator* uses protocol IMAP with TLS. If *Kerio Connect* is behind firewall, make sure the service is allowed. The IMAP service needs to be allowed on *Kerio Connect* server.

[3] Authentication details are used for the first connection to *Kerio Connect* and creation of a special account using JSON-RPC2 API for authentication. Once this special account is created, the PBX forgets the administrator's name and password.

17.4 Setting User PIN

User PIN used for login to voicemail box and email where voicemail messages are sent can be set as follows:

1. Go to *Configuration* → *Users*.
2. Select the user for whom you want to configure the voicemail.
3. Click on *Edit* or double-click the account.
4. This opens the *Edit user* dialog.
5. Go to the *Extensions* tab and set the PIN number.

Chapter 18

Setting Emergency Numbers

Kerio Operator allows you to create a list of emergency numbers. Such numbers can be dialled even if the users cannot call external network. It is also possible to change settings so that it is not necessary to use the dial-out prefix for these numbers.

Numbers can be set manually or predefined list of country numbers can be used.

To configure emergency calls, go to section *Configuration → Emergency Numbers* (see figure 18.1).

18.1 Adding Emergency Number

To add an emergency number manually, follow these instructions:

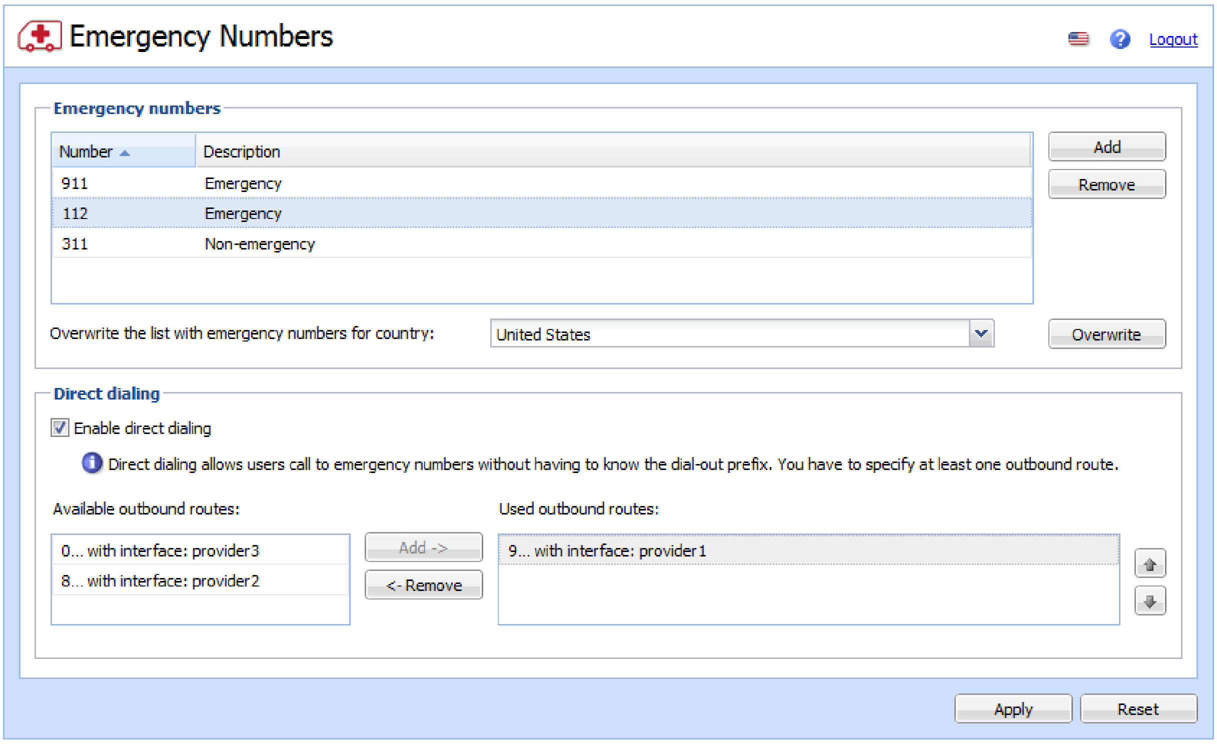
1. Click on *Add*.
2. Enter the telephone number in the *Number* column.
3. Write a short description in the *Description* column (see figure 18.1).

18.2 Preset List with Emergency Numbers

Kerio Operator has preset sets of emergency number for the following countries:

- Czech Republic,
- Germany,
- Slovakia,
- USA,
- United Kingdom.

To set emergency numbers for any available country in a single step, select the country from the list and click on *Rewrite* (see figure 18.1). Once you confirm, the numbers will be listed in the e,ergency numbers list. All previously configured number are rewritten but you can add more numbers manually (see section 18.1).



Emergency Numbers

Emergency numbers

Number	Description
911	Emergency
112	Emergency
311	Non-emergency

Overwrite the list with emergency numbers for country: United States

Direct dialing

☑ Enable direct dialing

Direct dialing allows users call to emergency numbers without having to know the dial-out prefix. You have to specify at least one outbound route.

Available outbound routes:

- 0... with interface: provider3
- 8... with interface: provider2

Used outbound routes:

- 9... with interface: provider1

Figure 18.1 Emergency Numbers

18.3 Direct Emergency Dialing

In *Kerio Operator*, all outgoing calls to external networks are realized with predefined prefix (for detailed information see chapter 6.6).

This implies that whenever a user with sufficient rights calls to an external network, they need to use the corresponding prefix.

You can configure an exception for emergency numbers

1. In section *Configuration* → *Emergency Numbers*, check the *Enable direct dialing* option.
2. Select at least one of the available outbound routes and use to the *Add* button to move it (see figure 18.1).

Warning:
Emergency numbers must no correspond with the internal extensions, otherwise users will reach the internal extensions in case of emergency. If the direct dialing is enabled, *Kerio Operator* does not allow creating extensions with the same numbers as emergency numbers.

Chapter 19

SSL Certificates

Kerio Operator allows communication encryption using SSL. The SSL encryption protocol first uses asymetrical encryption for exchange of symetrical key which is then used for encrypting the transmitted data. The asymmetric cipher uses two keys: a public one for encrypting and a private one for decrypting. As their names suggest, the public (encrypting) key is available to anyone wishing to establish a connection with the server, whereas the private (decrypting) key is available only to the server and must remain secret. The client, however, also needs to be able to identify the server (to find out if it is truly the server and not an impostor). For this purpose there is a certificate, which contains the public server key, the server name, expiration date and other details. To ensure the authenticity of the certificate it must be certified and signed by a third party, the certification authority.

Communication between the client and server then follows this scheme: the client generates a symmetric key and encrypts it with the public server key (obtained from the server certificate). The server decrypts it with its private key (kept solely by the server). This method ensures that the symmetric key is known only to the server and client.

Kerio Operator allows the use of certificates authenticated by a certificate authority and so-called self-signed certificates (certificates signed by themselves).

If you wish to obtain a "full" certificate you must contact a public certification authority (e.g. *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode*, etc.). The process of certification is quite complex and requires a certain expertise. *Kerio Operator* enables certification request that can be exported and the file can be delivered to a certification authority.

If you use self-signed certificate, it will be unique and issued by your company for your company for your server. This certificate ensures security for your clients as it explicitly shows the identity of your server. The clients will be notified by their web browsers that the certification authority is not trustworthy (when using the HTTPS protocol). However, since they know who created the certificate and for what purpose, they can install it. Secure communication is then ensured for them and no warning will be displayed again because your certificate has all it needs.

Self-signed certificate is created immediately during the first start of the PBX so that *Kerio Operator* can immediately communicate via encrypted SSL protocols. If needed, you can also generate your own self-signed certificate or you can prepare a certificate request and send it to a certification authority for verification, and then import it back to your PBX.

19.1 Creating Self-signed Certificate

To create a self-signed certificate, follow these instructions:

1. Go to section *Configuration → SSL Certificates* and click on *New → New Certificate*.
2. This opens a dialog where you enter the hostname of *Kerio Operator* server, the official name of your company, city and country where your company resides and hte period of validity. The *Hostname* and *Country* entries are required fields.
3. Save the certificate. When confirmed, the `server.crt` and `server.key` files are created under `sslcert`.

To enable the server to use this certificate, select the certificate and click on the *Set as Active* button.

19.2 Creating Certificate Signed by Certification Authority

If you wish to create and use a certificate signed by a trustworthy certification authority, follow these instructions:

1. Go to section *Configuration → SSL Certificates* and click on *New → New Certificate Request*.
2. This opens a dialog where you enter the hostname of *Kerio Operator* server, the official name of your company, city and country where your company resides and the period of validity. The *Hostname* and *Country* entries are required fields.
3. Save the request. When confirmed, the `server.crt` and `server.key` files are created under `sslcert`.
4. Select the certificate and click on the *Export* button. Save the certificate oo your disk and send it via email to a certification organization (for example, *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode* and so on).
5. Once you obtain your certificate signed by a certification authority, go to SSL certificate section and click on Import. Import the file.
6. To enable the server to use this certificate, select the certificate and click on the *Set as Active* button.

Chapter 20

Backup

Kerio Operator supports back-up of the following items:

- configuration file including all server and user accounts settings,
- voicmail boxes,
- SSL certificates,
- system logs,
- call logs,
- license.

In *Kerio Operator*, you can also perform a full restore from your backup.

20.1 Backup

To backup data of your PBX, go to section *Configuration* → *Advanced Options* to tab *Backup and Recovery*:

1. Check all the data types you wish to backup. We recomend to back your configuration after every complex change. Backup the voicemail boxes in regular intervals.
2. Click on *Create Backup*. Backup is performed any time in day while the server is running.
3. The *Download* button appears. Click the button and download the backup to your computer from which you connect to the PBX. Make sure you have enough free space on your disk or backup media before you start download.

20.2 Recovery

This operation requires PBX restart. If you run a call center, plan the recovery for time out of its peak hours. Expect a momentary breakdown.

You can recover your data into the same or higher version of *Kerio Operator*. Recovery to an older version will be refused due to data incompability.

To recover data of your PBX, go to section *Configuration* → *Advanced Options* to tab *Backup and Recovery*:

1. Click on *Upload Backup File*.
2. Upload this file to the system.
3. When the *Run Recovery* button appears, click on it.

Chapter 21

Product Upgrade

Whenever developers in *Kerio Technologies* prepare a new software version of *Kerio Operator*, a warning is displayed in *Kerio Operator Administration* (see chapter 3). Upload new version with a single click and everything is ready.

1. In *Kerio Operator Administration*, go to section *Configuration* → *Advanced Options* to tab *Product Upgrade*.

2. Click on *download*. A new version is downloaded into your computer from the *Kerio Technologies* server. Make sure you have enought free space on your disk.

3. On the *Upgrade Product* tab, click on *Upload Binary File*.

Chapter 22

Network Settings

Chapter *Network Settigns* describes various configuration settings of your PBX in the network.

22.1 Changing Network Settings

If you want to change network settings (for example, change IP address or set a static IP), go to section *Configuration → System*:

Changing IP address assigning

You can set a static IP address or let DHCP server handle the assigning. If users' telephones have a configured IP address instead of the DNS name of the PBX, we do not recommend to obtain IP address dynamically.

Changing IP address assigning can be done as follows:

1. In section *Configuration → System* in the *Ethernet Interfaces* table, double-click on the interface which *Kerio Operator* uses for communciation.
2. This opens dialog *Interface Properties* where can change the configuration. If you want your PBX to obtain address from a DHCP server,check the *Obtain configuration automatically via DHCP* Otherwise, select the *Use the following configuration* option and enter the IP address, mask and gate.

Setting DNS server address

Kerio Operator network settings should contain also the DNS server name. The server does not need a DNS name but we recommend to set one. During phone configuration, users prefer DNS name to IP address. DNS name is also necessary when the PBX uses dynamic IP address assigning via your DHCP server so that the PBX gets different IP addresses at a time. However, we do not recommend this option.

If you want to change the IP address of your DNS server or the method for assigning IP address of the DNS server (manually or via DHCP), go to section *Configuration → System*.

Network interfaces administration

All the network interfaces are displayed in section *Configuration* → *System* → *Network* in table *Ethernet interfaces*. The *Edit* button opens a dialog with a detailed information on the selected interface where you can change the configuration (configure IP address manually or obtain it via DHCP server).

Capturing network communication

Kerio Operator includes a tool for capturing network communication. This tool is useful especially in situations when connection to another SIP server fails or a phone cannot connect to the PBX.

To start capturing communication, follow these instructions:

1. In the administration interface, go to *Configuration* → *System*.
2. On the *Network* tab, click on *Advanced* → *Packet Sniffer*.
3. This opens a dialog where you can specify what to capture. You can capture communication in a single computer (by configuring its IP address) or you can specify individual ports.
4. Once the settings are done, click on *Start*.
5. Test the broken connection and click on the *Stop* button in the *Packet Sniffer* dialog.
6. In the same dialog, click on *Download* to download the file in your computer.
7. Open the file in an appropriate program (for example Wireshark).

22.2 Firewall

Kerio Operator allows you to limit or prohibit PBX services for certain networks. To configure backups, go to the *Firewall* tab under *Configuration* → *System*:

Before you configure this tab, it is necessary to decide on which hosts and subnets will be allowed to access the services. Then set correct IP groups. For more information on setting of IP address groups, refer to section 26.

Web server

If you want to limit possible connections to *Kerio Operator Administration* and *Kerio MyPhone*, check this option and select an IP group for addresses from which access will be allowed. Bear in mind that all the PBX users should be allowed to connect to *Kerio MyPhone* at least from their own workstation.

SIP

We recommend to limit the SIP protocol to you internal network and external IP addresses of your SIP provider.

Phone provisioning

For security reasons, we recommend to limit automatic phone provisioning to your internal network because TFTP sends configuration data as plain text.

Note: If the options are unchecked, no restrictions are set.

22.3 Time Settings

Correct time and tiem zone settings of your PBX are necessary for correct configuration of telephone communication, time ranges and logs. Therefore *Kerio Operator* is automatically synchronized with an NTP server.

NTP (Network Time Protocol) is a protocol for synchronizing time in your computer with time of the NTP server.

If you wish to change these settings, go to section *Configuration* → *System* tab *Time Settings*. Do not change the settings unless you have a good reason.

Chapter 23

User Rights

Kerio Operator allows to set various levels of user rights, for both system access or calls to specific numbers.

23.1 Roles for System Access

Kerio Operator distinguishes between the following roles:

- *No rights* — user has righs to access the *Kerio MyPhone* interface.
- *Whole server read only* — user has righs to access the *Kerio MyPhone* and and read only rights to *Kerio Operation Administration*.
- *Whole server read/write* — user has rights to access both the *Kerio MyPhone* and *Kerio Operation Administration* interfaces.

To change the user rights go to section *Configuration* → *Users* (see section 8.4)

Note: If you have assigned administration rights to one or more users, you can view changes they make in *Kerio Operator*. See the config log (see chapter 28).

23.2 Restrictions for Outgoing Calls

Some users can call private numbers or even premium rate lines during their office hours. To prevent this, you can simply block a number or a group of number for oneor more users. The number of such groups is not limited.

Each group is defined as either "all is permitted but the specified numberss" or, vice versa, "all is blocked but the specified numbers". You can even specifiy a group of user who can call only in your internal network (i.e. extension of other *Kerio Operator* users).

Groups for blocking calls are defined in section *Deinitions* → *Call Permission Groups*.

1. Click on *Add*.
2. In the *Add CAll Permission Group* dialog, enter the name and description for the group.
3. Click on *Add*.
4. Add a specific number or prefix and decide whether such number can be used or will be blocked.
5. Click OK to save the settings or repeat steps 3 and 4 for additional numbers.

Once all the rules are added, arrange them in order. If allowing calls to number 900123456 has a higher ranking that blocking prefix 900, user will be able to call number 900123456. If you change the order, blocking prefix 900 will be applied first and no other rules (situated under) called. Use the *Up* and *Down* buttons to adjust the order in the *Add Call Permission Group* table (see figure 23.1).

Once a group(s) is created, assign them to individual users (see section 8.4).

> ***Warning:***
> If you wish to limit calls to external network, bare in mind that external numbers in these definitions must include the prefix for outbound calls (see chapter 6.1).

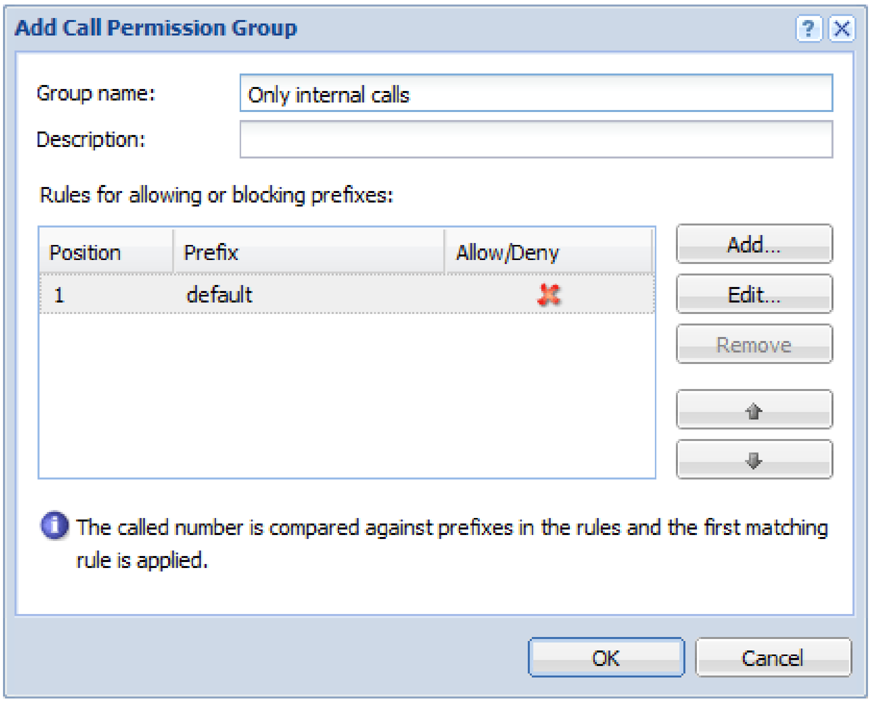
Usage of call persmission groups will be better understood through the following example where prefix for outboud calls is *0*:

Example — limiting calls to internal network

If you want to limit calls so that a certain group of users can call only within your internal network, follow these instuctions:

1. In section *Definitions* → *Call Permission Groups*, click on *Add*.
2. Enter the name for the group (for example, *Only internal calls* and a description.
3. In the *Add Call Permission Group*, double-click line *default* and change the rule to *Denied* (see figure 23.1).

Now outgoing calls are disabled and internal calls are automatically enabled. The restriction applies only to external interfaces.



Group name: Only internal calls

Description:

Rules for allowing or blocking prefixes:

Position	Prefix	Allow/Deny
1	default	✗

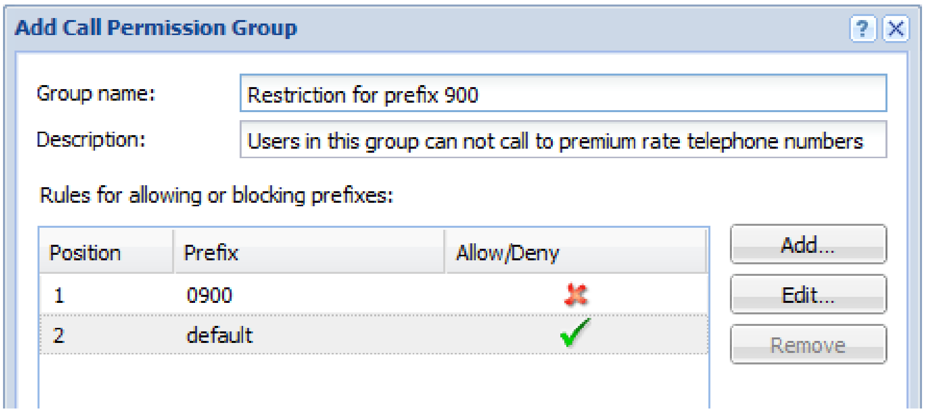
The called number is compared against prefixes in the rules and the first matching rule is applied.

Figure 23.1 Restrictions for Calls to Internal Network

Example — restrictions for calls to premium rate services

If you want to limit calls so that a certain group of users cannot call premium rate numbers (usuallay with prefix 900), follow these instuctions:

1. In section *Definitions* → *Call Permission Groups*, click on *Add*.
2. Enter the name for the group (for example, *Restriction for prefix 900* and a description.
3. n the *Add Call Permission Group*, double-click line *Add* and enter prefix 900 and the prefix for outgoing calls.
4. The final menu will look as the one in figure 23.2.



Group name: Restriction for prefix 900

Description: Users in this group can not call to premium rate telephone numbers

Rules for allowing or blocking prefixes:

Position	Prefix	Allow/Deny
1	0900	✗
2	default	✓

Figure 23.2 Call permission groups settings

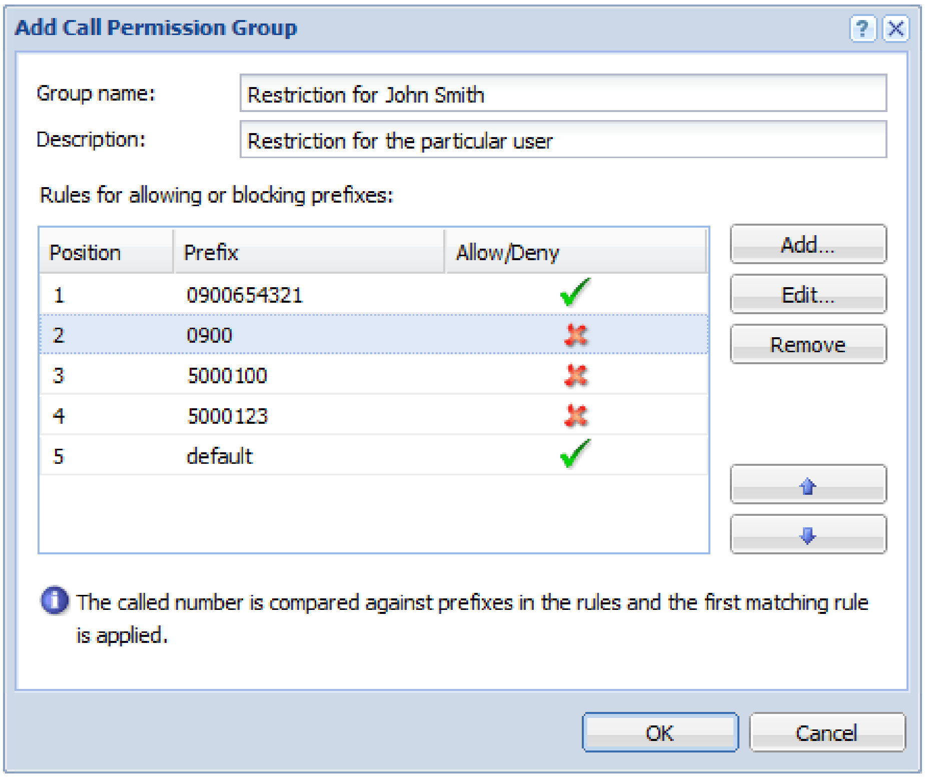
Example — restrictions for calls of a specific user

If you want to:

- allow a user to call to external network (allowing the default rule),
- deny calls to premium rate services (limit calls to prefix 900),
- deny calls to private numbers overused within office hours (specific numbers 555 0111 and 555 0222).
- allow calling number 900654321,

then follow these instructions:

1. In section *Definitions* → *Call Permission Groups*, click on *Add*.
2. Enter the name for the group (for example, *Restriction for John Smith* and a description.
3. Perform the settings in the previous example.
4. Click on *Add* and restrict the first phone number. Do the same for the second number.
5. Allow calling number 900654321 and move it above the rule restricking calls to prefix 900 by clicking *Up* (for the rule priority).



Group name: Restriction for John Smith

Description: Restriction for the particular user

Rules for allowing or blocking prefixes:

Position	Prefix	Allow/Deny
1	0900654321	✓
2	0900	✗
3	5000100	✗
4	5000123	✗
5	default	✓

The called number is compared against prefixes in the rules and the first matching rule is applied.

Figure 23.3 Call permission group settings for a specific user

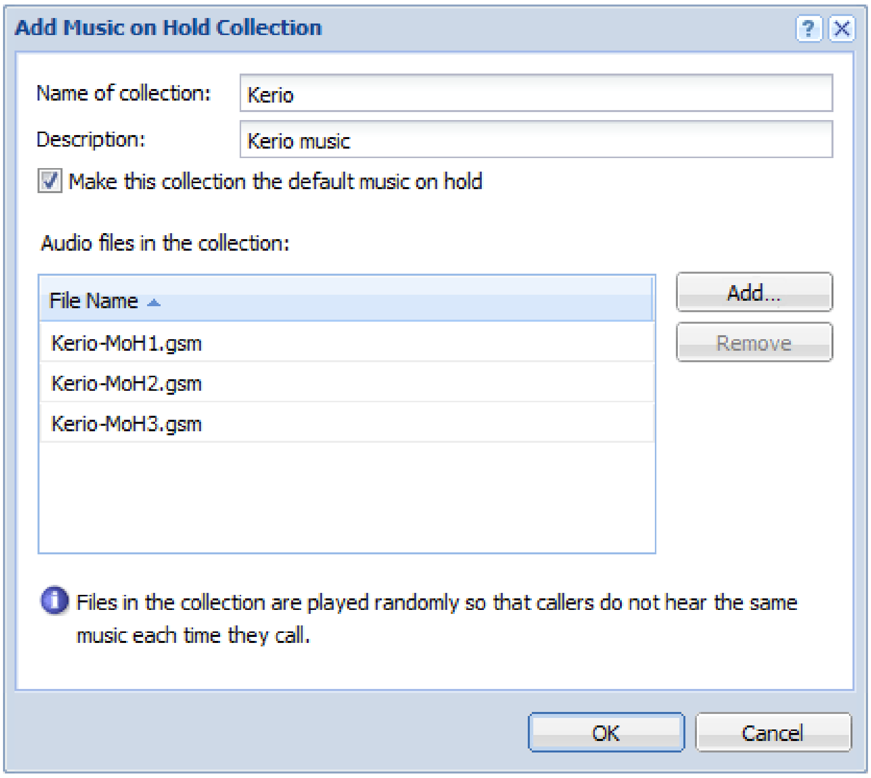
Chapter 24

Configuring Music on Hold

If a caller waits for connecting or in a call queue (see cahpter 14), they can hear recorded music. *Kerio Operator* has a default music collection. You can add and configure other audio files. You can upload any file in GSM and WAV format in section *Configuration* → *Definitions* → *Music On Hold*.

24.1 Adding New Collection

To add a new music collection (with one or more file), follow these instructions:



Add Music on Hold Collection

Name of collection: Kerio

Description: Kerio music

☑ Make this collection the default music on hold

Audio files in the collection:

File Name ▲
Kerio-MoH1.gsm
Kerio-MoH2.gsm
Kerio-MoH3.gsm

Files in the collection are played randomly so that callers do not hear the same music each time they call.

Figure 24.1 Adding New Collection

1. Go to *Configuration* → *Definitions* → *Music On Hold* and click on the *Add* button.

2. In the *Add Music on Hold Collection*, enter a name for the collection and a description.

3. Click on the *Add* button situated on the right side of the table with added audio files.

4. In the just displayed *Select Audio File* dialog, add file one by one by clicking *Upload*.

5. Select a file in the list and double-click it. Repeate this step until all your uploaded files are listed in table *Audio files in the collection* (see figure 24.1).

24.2 Setting Default Collection

In the *Add Music on Hold Collection* dialog, check the *Make this collection the default music on hold* to ensure this collection is used as default in all other *Kerio Operator Administration* settings.

The default collection is used while holding the line (usually the Hold button on most phones). The other collections can be used, for example, in call queues.

Chapter 25

Time Ranges

In the PBX, time ranges define time intervals for various scheduled operations (for example, for time condition applied in an auto attendant script — see section 16). They are not intervals in the true meaning of the word. They are a group containing any number of single or repeating time ranges.

Time intervals can be defined in the *Configuration* → *Definitions* → *Time Ranges* section.

Validity of Time Intervals

When defining a time interval three types of time ranges (subintervals) can be used:

Absolute
— interval has explicit start and end dates, it does not repeat

Weekly
— interval repeats every week (on selected days)

Daily
— interval repeats every day (in selected hours)

Note: If a certain time interval consists of multiple ranges of different types, it is valid in the time defined by the intersection of absolute ranges with the union of daily and weekly ranges. In symbols:
(d1 | d2 | w1 | w2) & (a1 | a2)
where
d1, d2 — daily ranges,
w1, w2 — weekly ranges,
a1, a2 — absolute ranges.

Defining Time Ranges

Time ranges will be best understood through the following example. Official working hours of the Sales Department in COMPANY are Monday to Friday, 9am to 5pm.

You can create time intervals in *Configuration* → *Definitions* → *Time Ranges* section:

1. Click on *Add*.
2. This open dialog *Add Time Range*. In section *Add to a group*, select the *Create new* option and enter a name for the new interval (for example, `Sales Department Office Hours`).
3. The *Description* is optional, for example *Weekdays from 9am to 5pm*.

4. Select `daily` in the *Type* menu and set the desired interval from 9 to 5 in the *From* and *To* fields.

5. In the *Valid on* menu, select *Weekdays*.

6. Click *OK*. to confirm changes.

Chapter 26

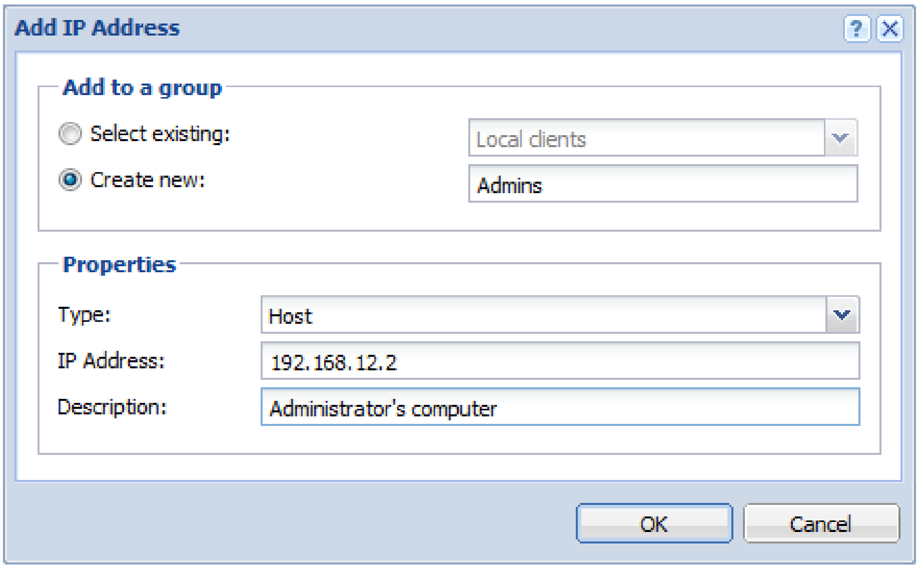
IP Address Groups

In the PBX, IP address groups define access to specific services (for example, access to *Kerio Operator Administration* or *Kerio MyPhone*). When setting access rights a group name is used. The group itself can contain any combination of computers (IP addresses), IP address ranges, subnets or other groups.

Creating groups

Creating a new group is best shown on an example. To create a new group of *Kerio Operator* administrators who can login to the *Kerio Operator Administration* interface from their own computers located in the local network only:

1. Click on *Add* in section *Configuration* → *Definitions* → *IP Address Groups*.
2. In the dialog for adding groups, select the *Create new* option and name it *Admins*.
3. In the *Type* menu, select the *Host* option.
4. In the IP address filed, enter the address of the PBX administrator's computer.
5. Add a description and save the settings (see figure 26.1).



○ Select existing: Local clients

● Create new: Admins

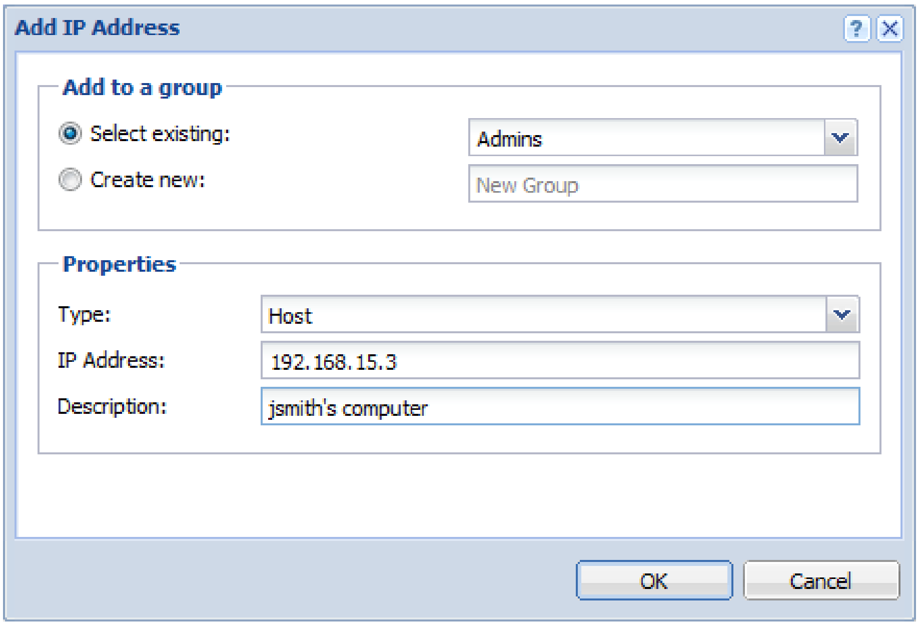
Type: Host

IP Address: 192.168.12.2

Description: Administrator's computer

Figure 26.1 IP Address Groups Creation

6. To add more PBX administrators, click on the *Add* button on the *IP Address Groups* tab. Select the existing group *Admins* (see figure 26.2).



Add IP Address

Add to a group

● Select existing: Admins

○ Create new: New Group

Properties

Type: Host

IP Address: 192.168.15.3

Description: jsmith's computer

Figure 26.2 IP Address Groups Creation

7. Repeat steps 3 and 4 for another computer in the group.

In our example, we added individual computers to a group. We can also add:

- Network — define network with an IP address and a mask
- IP address range — define the first and the last assigned IP address.
- Group — select an IP address group.

Chapter 27

Viewing PBX Status

When you are experiencing problems with your connection, we recommend to use tools for monitoring the status of your PBX. The tools are available in section *Status*:

27.1 Active Calls

All current calls can be viewed under *Status* → *Calls*.

This section displayed a table where each call occupies one line.

Go to section *Calls*, especially in case that you plan to restart the PBX which may result in an undesired termination of a call in progress.

27.2 Viewing Active Conferences

All current calls can be viewed under *Status* → *Conferences*. See chapter 13.3 for detailed information on viewing active conferences.

27.3 Viewing Call Queues

All current calls can be viewed under *Status* → *Call Queues*. See chapter 14.4 for detailed information on viewing active call queues.

27.4 System Health

The administration interface allows you to view the status of CPU, memory and disk space of your computer with *Kerio Operator*.

System status can be viewed under *Status* → *System Health*.

In this section, click on *Tasks* you can reboot or power off any planned tasks (see section 27.5) since they may burden your system.

The Support information link generates an asterisk configuration file and last 100 lines of all logs. This information may be helpful especially when solving issues in cooperation with the *Kerio Technologies* technical support.

See detailed information about disk space usage by clicking on *Details*. This open a dialog with information about disk usage of audio files, voicemail and configuration file of *Kerio Operator*.

27.5 Tasks

Scheduled tasks are system tasks which are carried out automatically in given intervals. Typical example of a scheduled task is a bulk removal of old recorded calls. Another example may be scheduled restart of automatically provisioned phones in case that parameters have been changed dramatically and it is necessary to restore configuration on all phones.

You can view scheduled tasks in section *Status* → *Tasks*.

Each line contains information about one task. Use the *Remove* button to remove any tasks.

27.6 Call History

The Call History section keeps a list of all internal and outbound calls of the PBX.

Call History can be viewed under *Status* → *Call History*.

Each line contains information about one call. The following actions can be applied to the call history:

Export to a CSV file

You can click on *Advanced* → *Export to a CSV file* to save the file on your local drive.

Clear

Click on *Advanced* → *Clear* and confirm your decision in the corresponding dialog.
Note: Individual users can delete their history in *Kerio MyPhone*. However, this operation only hides the data. They are not remove from the PBX and logs.

Chapter 28

Logs

Logs are files where information about certain events (e.g. error and warning reports, debugging information, etc.) are recorded. Each item is represented by one row starting with a timestamp (date and time of the event). Messages in logs are displayed in English for every language version of *Kerio Operator*.

28.1 Log settings

When you right-click inside any log window, a context menu will be displayed where you can choose several functions or change the log's parameters (view, logged information).

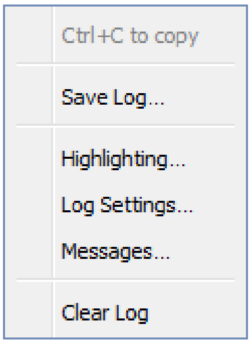


Figure 28.1 Context menu

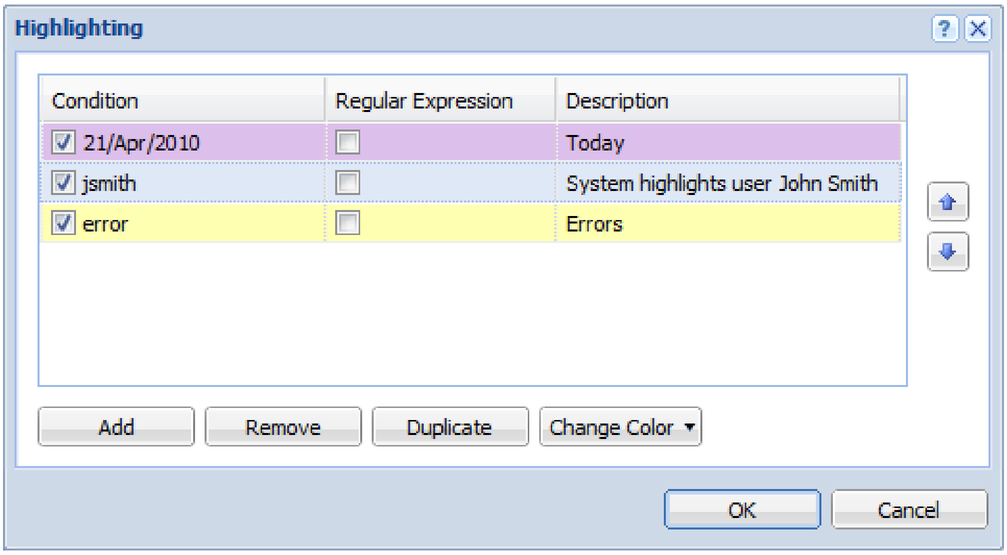
Save log

The Save log option enables saving of the entire log or its selected part in any file on the disk.
The dialog options are as follows:

- *Format* — the log may be saved as in plain text or in HTML. If the log is saved in HTML, the encoding and colors (where highlighting was used) will be saved.
- *Source* — the option enables saving of the entire log or a selected part of the text. The *Only selection* option is not active by default. Once a part of the text in the log is selected by the pointer, the option becomes active and the selected text can be saved.

Highlighting

Kerio Operator enables to highlight any part of text in logs. This function is used for better reference.
Click *Highlighting* to open a dialog box where highlighting can be added, changed and removed by using the typical *Add*, *Remove* and *Change Color* buttons.



Condition	Regular Expression	Description
☑ 21/Apr/2010	□	Today
☑ jsmith	□	System highlights user John Smith
☑ error	□	Errors

Figure 28.2 Highlighting

New highlighting can be set in the *Hghlighting* dialog box:

- *Condition* — every line containing the substring specified will be highlighted according to the parameters set in this dialog.
- *Regular extpression* — enter any regular expressions in the *Condition* field[4] (complex definition, for advanced users).
- *Description* — description used for better reference.

Every highlighting is applied to all log types. All lines meeting the condition are highlighted.

Log Settings

Select this option to open the Log debug dialog where you can set parameters for clearing or saving logs.

The File Logging tab

- *Enable logging to file* — enables logging to a specified file. Use the *File name* entry to specify a path where logs will be saved.
- *Rotate regularly*— select one of the following options:
  - *Every hour* — log is saved once an hour and a new log file is started.
  - *Every day* — log is rotated once a 24 hours.
  - *Every week* — log is rotated once a week.
  - *Every month* — log is rotated once a month.
- *Rotate when file size exceeds (MB)* — enter the maximum size of a log file (in MB).
- *Number of rotated log files to keep* — define how many log files will be stored. The oldest file will be cleared after each rotation.

External Logging

Open the *External Logging* dialog to set logging to a *Syslog* server or to a file. The three options can be combined.

[4] Regular expressions are special POSIX expression for a string description. They are created by various flexible patterns that are compared with strings.

- *Enable Syslog logging* — use this option to enable logging to a *Syslog* server
- *Syslog server* — DNS name or IP address of the particular *Syslog* server.
- *Facility*— — this entry helps *Kerio MailServer* recognize where a log came from (*Syslog* server can receive logs from various sources)
- *Severity* — set how important the log is (*Syslog* enables filtering of logs with respect to their severity).

Messages

This option is displayed only in the *Debug* log and allows you to configure logging information in detail.

Clear log

Selecting this option opens a warning dialog asking for your confirmation for clearing the log.

28.2 Config

The *Config* log includes all the history of communication with *Kerio Operator Administration*. It shows which user changed configuration and when.

The *Config* window contains three log types:

Information about logging in to *Kerio Operator Administration*

Example:

```
[11/Sep/2009 08:35:53] Admin - session opened for host 127.0.0.1
```

- `[11/Sep/2009 08:35:53]` — the date and time of the log creation
- `Admin` — the name of the user logged in for *Kerio Operator* administration.
- `session opened for host 127.0.0.1` — information about session opening and IP address of the user logged in

Changes in the configuration database

Changes performed in *Kerio Operator Administration*. See the creating of a new extension as an example:

```
[11/Sep/2009 08:35:53] Added extension 122 (ID=7)
```

- `[11/Sep/2009 08:35:53]` — the date and time of the log creation
- `Added extension 122 (ID=7)` — log entry.

28.3 Debug log

Debug log is a special log which can be used to monitor certain kinds of information, especially for problem-solving.

The *Debug* log displays many piece of information. Select those you need. Selection can be done as follows:

1. Right-click on the log screen and select option *Zprávy* in the context menu.
2. This opens dialog *Logging Messages* where you check the items which may help to solve your problem.

For communication problems, check `Asterisk` and `SIP protocol`.

Warning:
In addition, displaying too much information slows *Kerio Operator's* performance. We recommend that you only display information that you are interested in and only when necessary.

28.4 Error

In contrast to the *Warning* log, the *Error* log displays errors of great significance that usually affect the application's operation. The *Kerio Operator* administrator should check this log regularly and try to eliminate problems found here. Otherwise, users might have problems with some services or/and message loss and serious security problems might arise.

A typical error message in the *Error* log could be: a problem when starting a service (usually a collision at a particular port number), problems when writing to the disk or when authenticating an external user, etc.

28.5 Kernel

The *Kernel* log contains records generated by the operating system. It includes information about starting and stopping of the server, logs generated by individual processes, etc.

28.6 Security

The *Security* log records all attempts to access the administration interface.

28.7 Warning

The *Warning* log displays warning messages about errors of little significance. Typical examples of such warnings are messages stating that a user with administrator rights has a blank password or that an extension of a given number does not exist.

Events causing display of warning messages in this log do not greatly affect *Kerio Operator's* operation. They can, however, indicate certain (or possible) problems. The *Warning* log can help if for example a user is complaining that certain services are not working.

Chapter 29

Technical support

Kerio Technologies provides free email and telephone support for *Kerio Operator* to registered users. For contacts, see the end of this chapter. Our technical support staff is ready to help you with any problem you might have.

You can also solve many problems alone (and sometimes even faster). Please perform the following before you decide to contact *Kerio Technologies* technical support:

- Try to look up the answer in this manual. Its chapters describe the functions of *Kerio Operator* and how to use them for optimizing server settings in detail.
- If the answer cannot be found in this manual, refer to:
  1. the *Kerio Operator* website (http://www.kerio.com/),
  2. our technical support website (http://www.kerio.com/).
- Another useful information source is the discussion forum of *Kerio Operator* users — go to http://forum.kerio.com/ and the knowledge base that can be found on http://support.kerio.com/.
- Specific issues can be asked via a special technical support form at http://support.kerio.com/.

29.1 Contacts

USA

Kerio Technologies Inc.

2350 Mission College Blvd., Suite 400

Santa Clara, CA 95054

Phone: +1 408 496 4500

Email technical support is available at http://support.kerio.com/.

http://www.kerio.com/

United Kingdom

Kerio Technologies UK Ltd.

Enterprise House

Vision Park

Histon

Cambridge CB4 9ZR

Tel.: +44 1223 202 130, Fax.: +44 1223 233 055

Email technical support is available at http://support.kerio.com/.

http://www.kerio.co.uk/

Czech Republic

Kerio Technologies s.r.o.

Anglicke nabrezi 1/2434

301 49 PLZEN

Phone: +420 377 338 902

Email technical support is available at http://support.kerio.cz/.

http://www.kerio.cz/

Russian Federation

Kerio Technologies Russia

Bersenevskaja Quay, b. 20/2

Office 518

119 072 Moscow

Tel.: +7 (495) 9593062, Fax: +7 (495) 9593062

http://www.kerio.ru

Appendix A

Legal Notices

Internet Explorer® and Active Directory® are registered trademarks of Microsoft Corporation.

Cisco® and Linksys® are registered trademarks of Cisco Systems, Inc.

Digium® and Asterisk® are registered trademarks of DigiumInc.

snom® is registered trademark of snom technology AG.

VMware® is registered trademark of VMware, Inc.

Safari™ and Open Directory logo™ are trademarks of Aple Inc.

Wireshark® is registered trademark of Wireshark Foundation.

Firefox® is registered trademark of Mozilla Foundation.

Appendix B

Used open source software

Used open source software

This product contains the following open-source libraries:

Appliance OS Sources

Kerio Operator devices are based on open software from various resources. For detailed information on conditions of each particular software used in the product, refer to `/opt/kerio/operator/doc/Acknowledgements`
To download the source package, go to http://download.kerio.com/archive/.

bluff

Bluff is a JavaScript port of the Gruff graphing library for Ruby.
Copyright (c) 2008-2009 James Coglan
Original Ruby version (c) 2005-2009 Topfunky Corporation boss@topfunky.com

excanvas

Firefox, Safari and Opera 9 support the canvas tag to allow 2D command-based drawing operations. ExplorerCanvas brings the same functionality to Internet Explorer.
Copyright © 2006 Google Inc.

fbexport

Kerio Operator contains a modified version of fbexport. It is distributed under the terms of Mozilla Public License.
Download the modified cersion at http://download.kerio.com/archive/.

Heimdal Kerberos

Heimdal is an implementation of Kerberos 5, largely written in Sweden. It is freely available under a three clause BSD style license (but note that the tar balls include parts of Eric Young's libdes, which has a different license). Other free implementations include the one from MIT, and Shishi. Also Microsoft Windows and Sun's Java come with implementations of Kerberos.
Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.
Copyright ©1995-1997 Eric Young. All rights reserved.
Copyright ©1990 by the Massachusetts Institute of Technology
Copyright ©1988, 1990, 1993 The Regents of the University of California. All rights reserved.
Copyright ©1992 Simmule Turner and Rich Salz. All rights reserved.

ctype.h

The ctype.h library for the C programming language contains declarations for character classification features.
Copyright ©2000-2002 The Apache Software Foundation.

libcurl

Libcurl is a free and easy-to-use client-side URL transfer library. It supports the following protocols: FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP.
Copyright ©1996-2008, Daniel Stenberg.

libiconv

Libiconv converts from one character encoding to another through Unicode conversion.
Copyright ©1999-2003 Free Software Foundation, Inc.
Author: Bruno Haible
Homepage: http://www.gnu.org/software/libiconv/
The *libiconv* library is distributed and licensed under GNU Lesser General Public License version 3.
Kerio Operator includes a customized version of this library. Complete source codes of the customized version of *libiconv* library are available at:

http://download.kerio.com/archive/

libmbfl

libmbfl is a streamable multibyte character code filter and converter library. The *libmbfl* library is distributed under LGPL license version 2.
Copyright ©1998-2002 HappySize, Inc. All rights reserved.
The library is available for download at:

http://download.kerio.com/archive/

libxml2

XML parser and toolkit.
Copyright ©1998-2003 Daniel Veillard. All Rights Reserved.
Copyright ©2000 Bjorn Reese and Daniel Veillard.
Copyright ©2000 Gary Pennington and Daniel Veillard
Copyright ©1998 Bjorn Reese and Daniel Stenberg.

Net_SMTP PEAR module

Net_SMTP PEAR module is a PEAR library implementing the SMTP protocol.
Copyright ©1997-2003 The PHP Group

Net_Socket PEAR module

Net_Socket PEAR module is a Network Socket Interface PEAR library.
Copyright ©1997-2003 The PHP Group

OpenLDAP

Freely distributable *LDAP* (*Lightweight Directory Access Protocol*) implementation.
Copyright © 1998-2007 The OpenLDAP Foundation

Copyright ©1999, Juan C. Gomez, All rights reserved
Copyright ©2001 Computing Research Labs, New Mexico State University
Portions Copyright©1999, 2000 Novell, Inc. All Rights Reserved
Portions Copyright ©PADL Software Pty Ltd. 1999
Portions Copyright ©1990, 1991, 1993, 1994, 1995, 1996 Regents of the University of Michigan
Portions Copyright ©The Internet Society (1997)
Portions Copyright ©1998-2003 Kurt D. Zeilenga
Portions Copyright ©1998 A. Hartgers
Portions Copyright ©1999 Lars Uffmann
Portions Copyright ©2003 IBM Corporation
Portions Copyright ©2004 Hewlett-Packard Company
Portions Copyright ©2004 Howard Chu, Symas Corp.

OpenSSL

An implementation of *Secure Sockets Layer* (SSL v2/v3) and *Transport Layer Security* (TLS v1) protocol.
This product includes software developed by the *OpenSSL Project* for use in the *OpenSSL Toolkit* (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young.
This product includes cryptographic software written by Tim Hudson.

PEAR — PHP Extension and Application Repository

PEAR is a framework and distribution system for reusable PHP components.
Copyright ©1999-2006 The PHP Group. All rights reserved.

PHP

PHP is a widely-used scripting language that is especially suited for Web development and can be embedded into HTML.
Copyright ©1999-2006 The PHP Group. All rights reserved.
This product includes PHP software, freely available from http://www.php.net/software/

Ralink (firmware) Debian non-free package

Binary firmware for Ralink RT2561, RT2571, RT2661 and RT2671 wireless cards.
Copyright ©2007, Ralink Technology Corporation

tftpd

TFTP daemon. TFTP is a simple protocol used for file transmission.
Copyright ©1983 Regents of the University of California. All rights reserved.

zlib

General-purpose library for data compressing and decompressing.
Copyright ©1995-2005 Jean-Loup Gailly and Mark Adler.

Glossary of terms

Firewall

Software or hardware device that protects a computer or computer network against attacks from external sources (typically from the Internet).

IP

IP (Internet Protocol) is a protocol which uses its data part to convey all the other protocols. The most important information in its header is the source and destination IP address, i.e. by which host the packet was sent and to which host it should be delivered.

IP address

IP address is a unique 32-bit number used to identify the host in the Internet. It is represented by four bytes in the decimal system (0–255) separated by dots (e.g. `200.152.21.5`). Each packet includes the information on where the packet was sent from (source IP address) and to which host it should be delivered (destination IP address).

Kerberos

Protocol for secure user authentication in network environments. It was designed by MIT (Massachusetts Institute of Technology) within the Athena project. The protocol is based on such principles where the third side is trustworthy. Users use their passwords to authenticate to the central server (KDC, Key Distribution Center) and the server sends them encrypted tickets which can be used to authenticate to various services in the network.

LDAP

LDAP (Lightweight Directory Access Protocol) is an Internet protocol used to access directory services. Information about user accounts and user rights, about hosts included in the network, etc. are stored in the directories. Typically LDAP is used by email applications to search for email addresses and to delivery management (*Microsoft Active Directory*).

Port

16-bit number (1–65535) used by TCP and UDP for application (services) identification on a given computer. More than one application can be run at a host simultaneously (e.g. web server, mail client, web client — web browser, FTP client, etc.). Each application is identified by a port number. Ports 1–1023 are reserved and used by well known services (e.g. 80 = WWW). Ports above 1023 can be freely used by any application.

RFC

RFC (Request For Comments) is a set of deliberately recognized standards. It is a set of indexed documents where each document focuses a particular area of network communication.

Subnet mask

Subnet mask divides an IP address in two parts: network mask and an address of a host in the network. The mask has the same format as IP addresses (e.g. 255.255.255.0), but it is displayed as a 32-bit number with certain number of left-to-right oriented ones and zeros (mask cannot include other values). Number one in a subnet mask represents a bit of the network address and zero stands for a host's address bit. All hosts within a particular subnet must have identical subnet mask and network part of IP address.

Index