Kerio Operator

Administrator's Guide

Kerio Technologies

This guide provides detailed description on *Kerio Operator*, version *1.2.1*. 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 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 appliance.

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

2.1 Product Editions

Kerio Operator is available in these editions:

Software Appliance

Kerio Operator Software Appliance (so called software appliance) is an all-in-one package of *Kerio Operator* which also includes a special operating system.
Designed to be installed on a computer without an operating system, this edition is distributed as an installation disc. *Software Appliance* cannot be installed on a computer with another operating system and it does not allow to install other applications.

VMware Virtual Appliance

A virtual appliance designed for usage in *VMware* products.
VMware Virtual Appliance is a *Software Appliance* edition pre-installed on a virtual host for *VMware*. The virtual appliance is distributed as *OVF* and *VMX*.

Kerio Operator Box

Hardware device ready for network connection. There are two types which differ in performance.

2.2 Kerio Operator Software Appliance

For Kerio Operator system requirements, refer to the Kerio Operator product pages.

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 application is also installed during the process.

2.2.1 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 by a firewall and supporting security rules, your internal telephone extension can be misused which may result in unexpected financial costs.

2.3 Kerio Operator VMware Appliance

For supported VMware products, refer to the Kerio Operator product pages.

Use an installation package in accordance with the type of your VMware product:

- In case of products *VMware Server, Workstation* and *Fusion*, download the compressed *VMX* distribution file (`*.zip`), unpack it and open the file with extension `.vmx`.
- You can import a virtual appliance directly to *VMware ESX/ESXi* from the URL of the *OVF* file — for example:

  ```
  http://download.kerio.com/cz/dwn/operator/
  kerio-operator-appliance-1.2.0-2500-linux.ovf
  ```

  VMware ESX/ESXi automatically downloads the *OVF* configuration file and a corresponding disk image (`.vmdk`).

If you import virtual appliance in the *OVF* format, bear in mind the following specifics:

- In the imported virtual appliance, time synchronization between the host and the virtual appliance is disabled. However, Kerio Operator features a proprietary mechanism for synchronization of time with public Internet time servers. Therefore, it is not necessary to enable synchronization with the host.
- Tasks for shutdown or restart of the virtual machine will be set to default values after the import. These values can be set to “hard” shutdown or “hard” reset. However, this may cause a loss of data on the virtual appliance. *Kerio Operator VMware Virtual Appliance* supports so called *Soft Power Operations* which allow to shut down or restart hosted operating system properly. Therefore, it is recommended to set shutdown or restart of the hosted operating system as the value.

For more information, go to section 2.2.1.

2.4 Kerio Operator Box

For currently supported Kerio Operator Box configurations, refer to the Kerio Operator product pages.

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

2.4.1 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 change the configuration.
- in the administration in section *System* — after you 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`

To shut down the appliance:

1. Connect to Kerio Operator via the console and select the `Shutdown` command.
2. Kerio Operator series 1000 will shut down.

   Kerio Operator series 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* button 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 to use the supported browsers to connect to the interfaces. For the list of the browsers, refer to the Kerio Operator product pages.

Web interfaces are currently localized into several languages. Select yours in the top right corner of the 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 4021. 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.name:4021/admin`

in case your computer does not have a DNS record:

`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 certificate (for more information, see chapter 22). Since you know the certificate can be trusted, you can add the security exception and continue to a login page.

First login

When you connect to the PBX for the first time, a configuration wizard is displayed where you:

1. Set the configuration wizard language.
2. Accept the Kerio Operator license agreement.
3. Set a password for the administration account (be sure to remember the password, you will need it to login to the PBX).

Note: This administrator's password is synchronized with the password of user root in the operating system.

4. Set the time zone of Kerio Operator (requires a restart of the PBX).
5. Set the PBX language for communication with you and other users (warnings, auto attendant scripts, voicemail, etc.).

After successful configuration, the login page is displayed. Enter the username and password you created earlier (see figure 3.1).

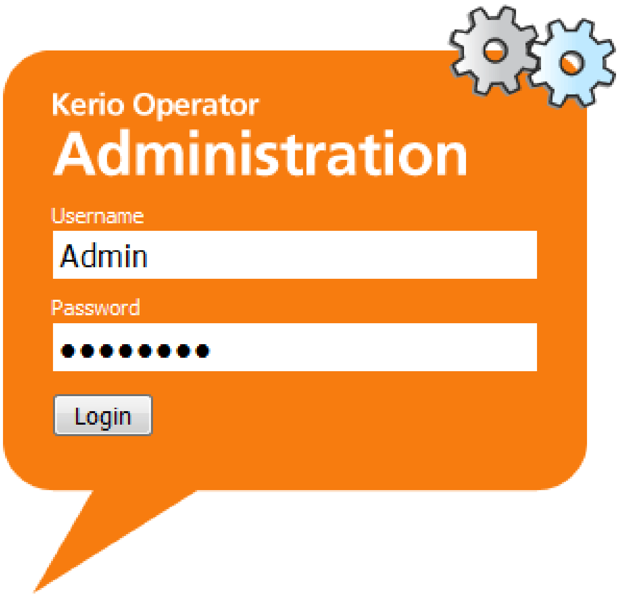

Figure 3.1 Login to administration

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 are logged in with and double-click on it.
4. Change the password on tab *General*.

3.2 Kerio MyPhone

With Kerio MyPhone, users can access their voicemail, account configuration and call history. They can also use it to make calls to internal extensions of Kerio Operator. To make calls, a softphone is required.

`http(s)://kerio.operator.name`

If the URL is entered correctly, *Kerio MyPhone* login page is displayed (see figure 3.2).

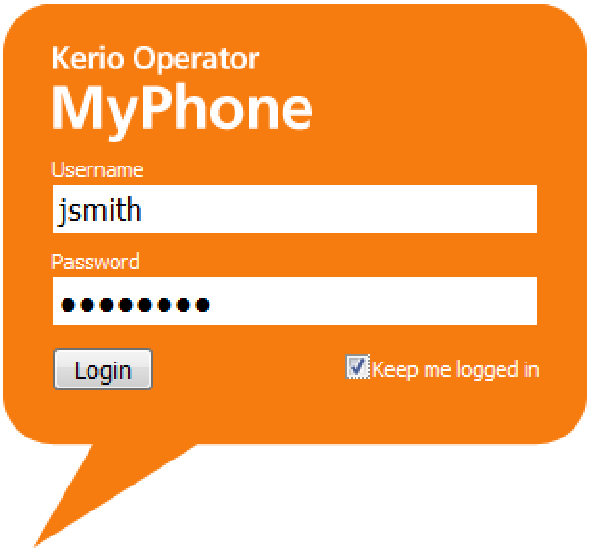

Figure 3.2 Login to Kerio MyPhone

3.3 Context Help

The Kerio Operator web interface 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 (figure6.7).

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 a certain 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 chapter 4.3.

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

4.2 Registration the Product in the Administration Interface

You can register the product from the welcome page of the administration interface (see figure 4.1) which is displayed after each login.

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).

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 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 in the administration interface.

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.

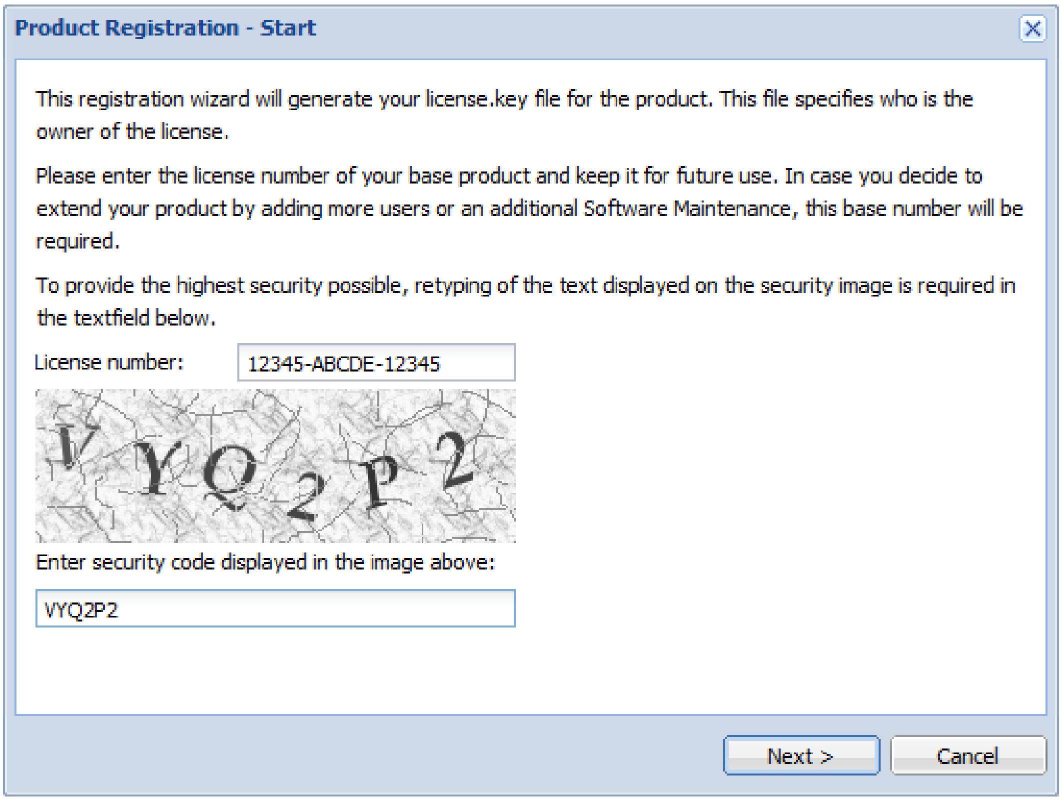

Figure 4.2 License number

   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 performing registration of 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 welcome 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.

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.

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 colored 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/.

4.5 Communication with Kerio Technologies

You can communicate with Kerio Technologies directly from Kerio Operator. You can provide Kerio Technologies with the following information:

- suggestions to improve the product — write the suggestion in the suggestion forum. The *Suggest idea* button opens a dialog where we recommend you to enter your email address so that we can inform you about any progress. After that, the suggestions forum is opened.

Note: If the page is not opened, allow pop-up windows for the Kerio Operator page.

- reporting technical problems with Kerio Operator — problems will be reported once you have configured SMTP server in section *Advanced Options* → *General*.

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.
- Communication in the internal firewall of the PBX should be limited. To configure it, go to the *Firewall* tab under Configuration *System*→ *Firewall*.
- Strong SIP passwords should be set (do not use dictionary words, they should have more than eight characters and the password should contain three types of characters — letters, numbers and special symbols).
- Number of attempts to enter SIP password should be limited.
- We recommend using special rules to disable international calls to countries which you do not call or disable international calls for employees who are not expected to call abroad. To configure it, go to the *Configuration* → *Definitions* → *Call Permissions Groups*:
- We recommend to limit outgoing calls to countries which you rarely call in section *Configuration* → *Advanced Options* → *Security*.

The following sections describe these settings in detail.

5.1 How to configure firewall in local network

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 if integration with Kerio Connect is enabled and there is a firewall between Kerio Connect and Kerio Operator.	deny
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* from the Internet.
HTTPS (4021)	allow	allow if you wish users to be able to connect to the administration interface from the Internet.

Table 5.1 Services to be allowed on the firewall

5.2 Integrated Firewall Configuration

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 30.

Web server

If you want to restrict connections to Kerio Operator Administration and Kerio MyPhone, check this option and select an IP group with 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 restrict the SIP protocol solely to your internal network and external IP addresses of your SIP provider.

Phone provisioning

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

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

5.3 Setting protection against password guessing

Login data guessing is one of the most common attacks on a PBX. In Kerio Operator, attackers try to guess extension numbers and SIP passwords. This type of attack is defined by many unsuccessful attempts to enter extension number and SIP password during a login. Kerio Operator security settings enable you to limit the number of attempts of a phone (both software and hardware) to connect to the PBX. Apply settings as described below:

1. In the administration interface, go to *Configuration* → *Advanced Options* → *Security*.
2. Set the limit of unsuccessful attempts (usually 3 to 10 attempts) and set the time period during which attempts will be counted.

   Setting the time period protects real users who have forgotten their password or who have made mistakes during several logins. When the time limit expires, they can try to login to the PBX again.
3. Now define the action which will be performed when the conditions are met. The PBX will block the source IP address for the set time period. You can select whether the time period will be in minutes, hours or days.
4. You can also enter your email to be notified if an IP address is blocked.

How to recognize there has been an attack attempt

Look for the `Authentication failed` string in the *Security* log. If there are many messages of this kind, somebody is trying to use a dictionary attack.

5.4 How to use prefixes to disable outgoing calls of individual users

Although you pay attention to the security of your PBX, there is still a chance an attacker will break through your security and obtains the number of an internal extension and its SIP password. They may use phone or email to contact the users and elicits their usernames and passwords. Viruses which are installed in users' computers and send usernames and passwords to the attacker are another threat.

The attacker obtains username and password and establishes phone services with premium numbers (usually in a country where such fraudulent behavior is not illegal). They then use your PBX to call these premium rate numbers. Thus you can lose a large amount of money.

If an attacker obtains a username and password of one of your users, we recommend to have configured restrictions for outgoing calls. Disable calls to countries where users never call.

Since you may have employees with different needs, you can create call permission groups to external networks and assign them to users according to their needs.

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

Groups whose calls are blocked are defined in section *Definitions* → *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 ??).

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, beer in mind that external numbers in these definitions must include the prefix for outbound calls (see chapter 6.1).

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

Example — disabling international calls

Suppose we have a company based in the USA. One group of employees can make outgoing calls but they can only make calls to Mexico:

- the prefix for calling to external network must be a part of the string (in our case, it is 9)
- all international prefixes (00) are forbidden
- enable the prefix for Mexico — 0052 (including the prefix for calling external network — 90052)

Apply settings as described below:

1. In section *Configuration* → *Definition* → *Call Permission Groups*, click on *Add*.
2. Enter the name for the group (for example, *International calls disabled*) and a description.
3. In dialog *Add Call Permission Group*, click on *Add* and enter the prefix for international calls 00 together with your prefix for calls to external networks which is 9. The result is 900.
4. Set the rule to *Deny*.
5. To allow calls to Mexico, we must add another rule. This rule allows calls to prefix 0052.
6. Figure 5.1 shows the example of the final configuration.

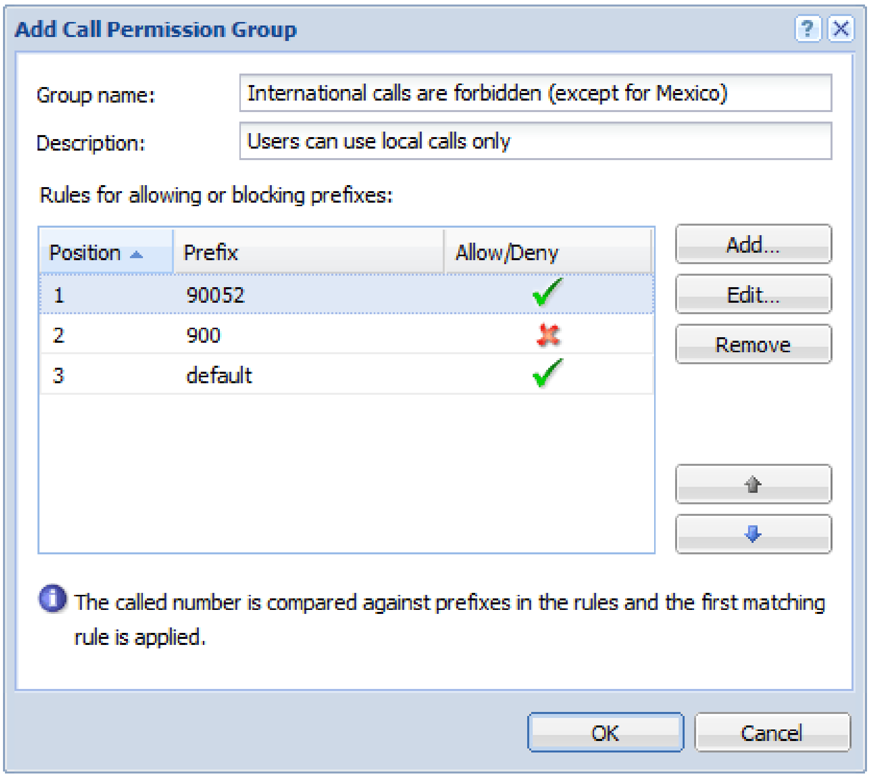

Figure 5.1 Call permission groups settings

> ***Warning:***
> The rules are applied in order, one by one, so bear this in mind when creating permission groups.

5.5 Settings constraints for outgoing calls

Apart from completely disabling calls to certain countries (see section 5.4), you can also limit outgoing calls. You can limit the duration and number of the calls. Use these limitations when you cannot disable calls to a specific country completely but want to protect yourself.

You can set constraints to:

- calls to all countries where you do not do business (this problem can be easily solved with Call Permission Groups — see section 5.4),
- long international calls — regular calls do not last for hours,
- too many concurrent calls.

First and the easiest option is to limit the maximum duration of every call. Maximum call duration can be done as follows:

1. Open the *Configuration* → *Advanced Options*→ *Security* section.
2. Adjust the settings in *Maximum duration of each outgoing call* according to your needs.

Other option is to configure special rules for restricting outgoing calls in section *Configuration* → *Advanced Options* → *Security* in table *Outgoing calls constraints*:

The table lists one rule which limits all outgoing calls to 50 per hour and total call duration to 2 hours per day.

Usage of rules is best shown on an example:

- The rule will be configured for a manufacturer who sells and has contacts in the USA and EU. This means that we cannot limit prefixes for the USA and Europe but we can set limits to calls to other countries.
- Prefix for calls to external network is `9` (prefix is configured in section *Configuration* → *Call Routing*).

Create the rule as described below:

1. Go to section *Configuration* → *Advanced Options* → *Security* and add a new item in table *Outgoing call constraints*.
2. This opens the *Add Outgoing Call Constraint* dialog.
3. Enter a name for the rule (for example `Restrictions for all countries except the USA and EU`).
4. In section *Apply to these outgoing calls*, select *All except listed* and click on *Add*.

5. This opens the *Add Outgoing Call Prefix* dialog, with an example on using prefixes.

   International prefixes can be found, for example, on Wikipedia.

   Each international call prefix should be preceded by your prefix for outgoing calls. In this case, the prefix is 9.

   For our scenario, enter prefix 9001 (001 for Northern America), 9003 and 9004 (003 and 004 for Europe).

6. Now define the constraint. Limit *Maximum call count* to 10 per hour and *Maximum total calls duration* to 1 hour per day.

7. Select an action which will be performed when the conditions are met. You can configure either sending of a warning email or blocking of outgoing calls (which means that nobody will be able to call to external network).

   The optimum use of these rules is as follows: Create one soft rule with lower limits which will send warning messages via email and one other rule with higher limits which will block the PBX.

   > ***Warning:***
   > If the limits are reached and the PBX is blocked, nobody will be able to make calls to external network. The PBX can be unlocked in section *Configuration → Advanced Options → Security*. Therefore we recommend to make a thorough analysis of your calls so that the PBX is not blocked by legal operations.

Besides standard security rules which are configured to be used against attackers, you can set similar rules for specific users or groups of users. To do this, go to section *Call Permission Groups*. For more information about such rules, see chapter 27.1.

> ***Warning:***
> Introduce the limitations to your Kerio Operator users. You can also consult the settings with your company management.

How to defend yourselves against attacks

In case of an attack, apply the following instructions as soon as possible:

1. See section *Status → Calls* and logs and find out which user account was abused.

2. Change the SIP password of this account.

3. Instruct users about handling their login details and secure behavior on the Internet.

4. The PBX is blocked, so it needs to be unlocked again.

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 outgoing 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 to know:

- telephone number or numbers from 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 connect to your provider's SIP server.

1. In the administration 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 must not contain spaces, national and special characters and must be unique.
3. Select the *New provider* option. The configuration differs for settings with 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 operator 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 *Required to register with Registrar* option, the first time registration to a SIP server is required by the majority of providers.

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

   Note: Some registrars that require these settings do not allow hiding phone numbers (extensions settings: *Configuration → Extensions → Add/Edit extension dialog → Advanced tab*).

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 operator who will direct all external calls made to 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 *Required to register with Registrar* option, the first time registration to a SIP server is required by the majority of providers.

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

Note: Some registrars that require these settings do not allow hiding phone numbers (extensions settings: *Configuration* → *Extensions* → *Add/Edit extension dialog* → *Advanced tab*).

8. Save the settings.
9. 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).

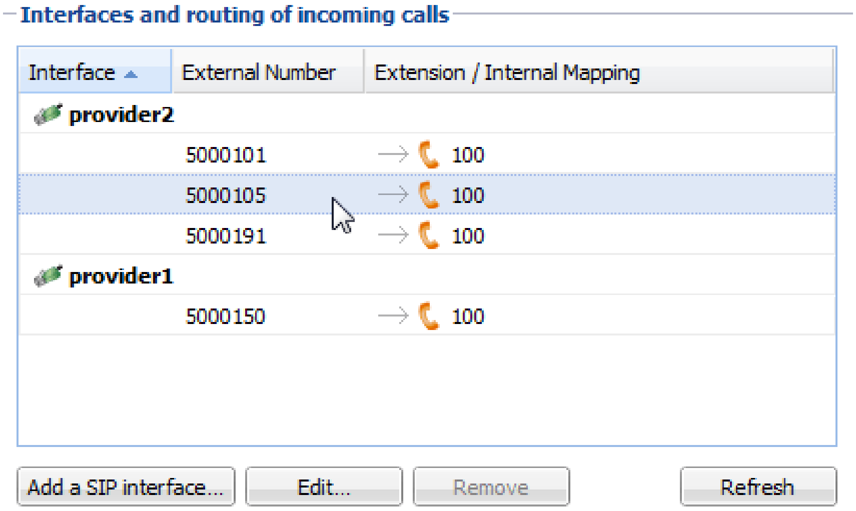

Figure 6.1 Mapping individual numbers to internal extensions of Kerio Operator

10. 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.

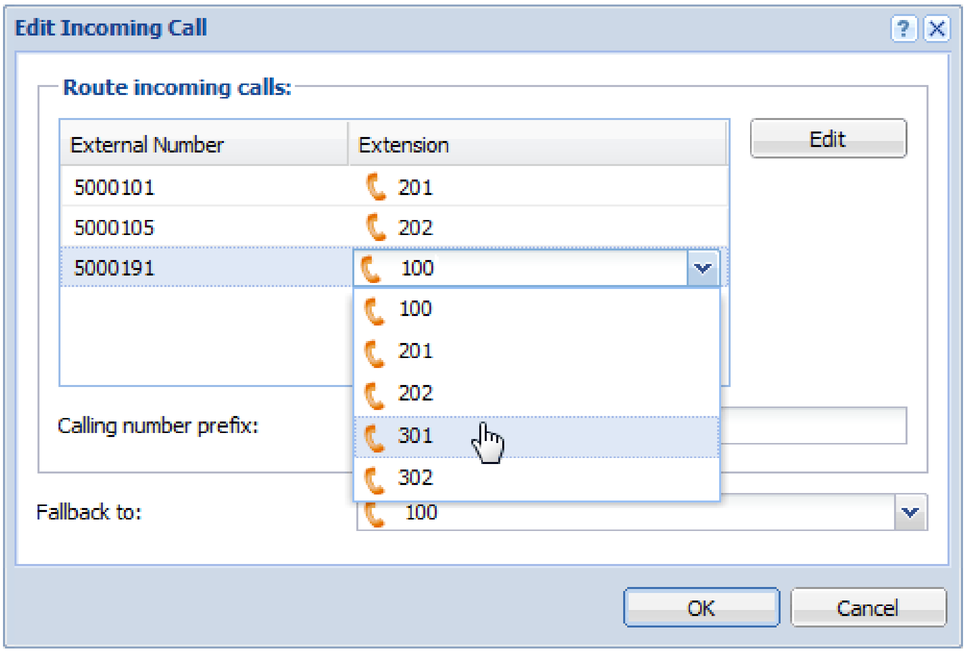

Figure 6.2 Mapping individual numbers to internal extensions of Kerio Operator

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 *Required to register with Registrar* option only if the provider requires registration. With large number intervals (so called “trunks”), providers usually do not require registration. The registration is replaced by an IP address of Kerio Operator. The address must be fixed and the provider needs to know about any changes.
8. If the user ID differs from the telephone number, type it in the user ID field.

   Note: Some registrars that require these settings do not allow hiding phone numbers (extensions settings: *Configuration* → *Extensions* → *Add/Edit extension dialog* → *Advanced tab*).
9. Click *OK* to confirm settings.
10. Finally, 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 administration 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 must not 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 other server uses extensions 3XX), all 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 communicates.

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

8. If the server requires registration, check the *Required to register with Registrar* option.

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

10. Click *OK* to confirm settings.

11. Finally, 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, a rewriting 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. The rewriting 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.

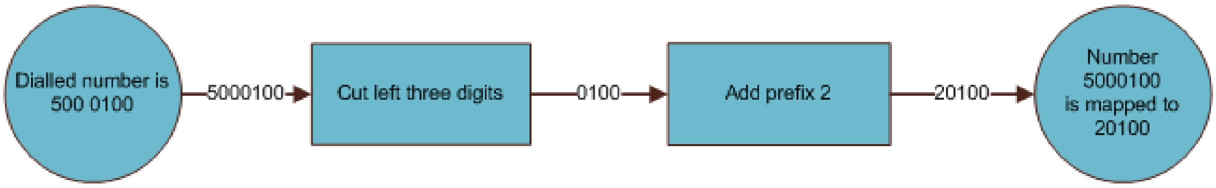

Figure 6.3 Rewriting rule for number 123456789

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.

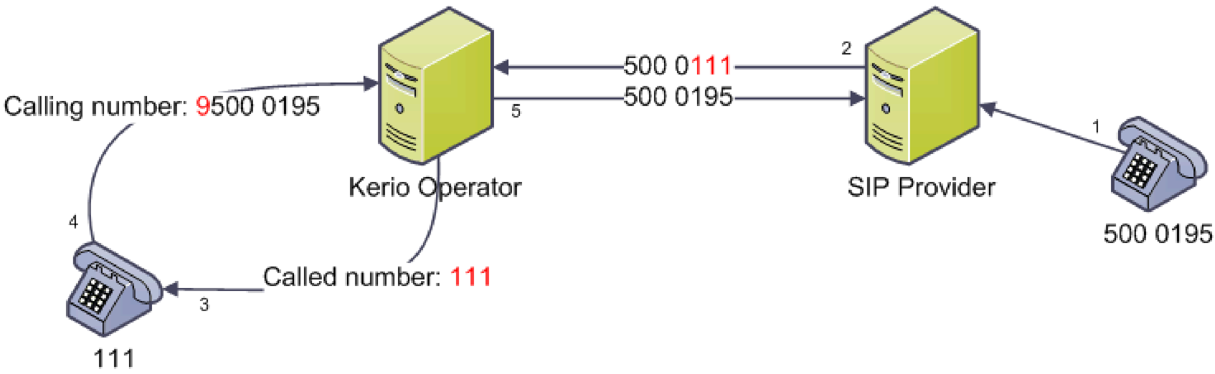

Figure 6.4 Incoming and answer call (read from right to left)

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).

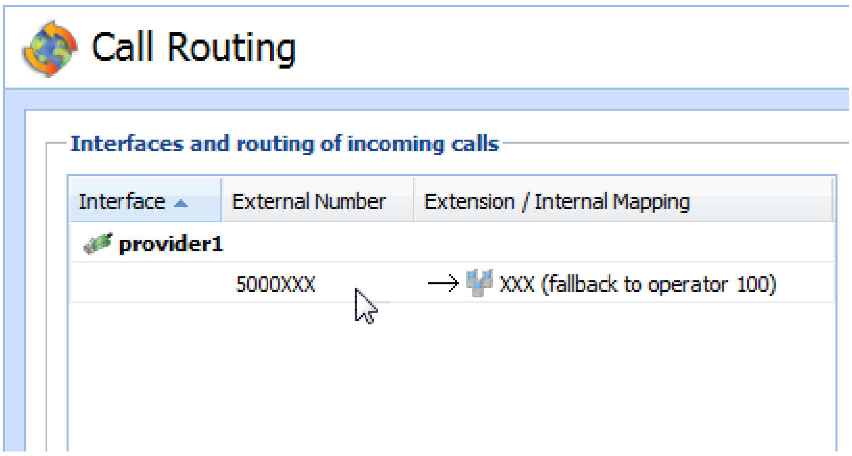

Figure 6.5 Rule for interface provider1

2. This displays the *Edit incoming Call* dialog (see figure 6.6). 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.

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

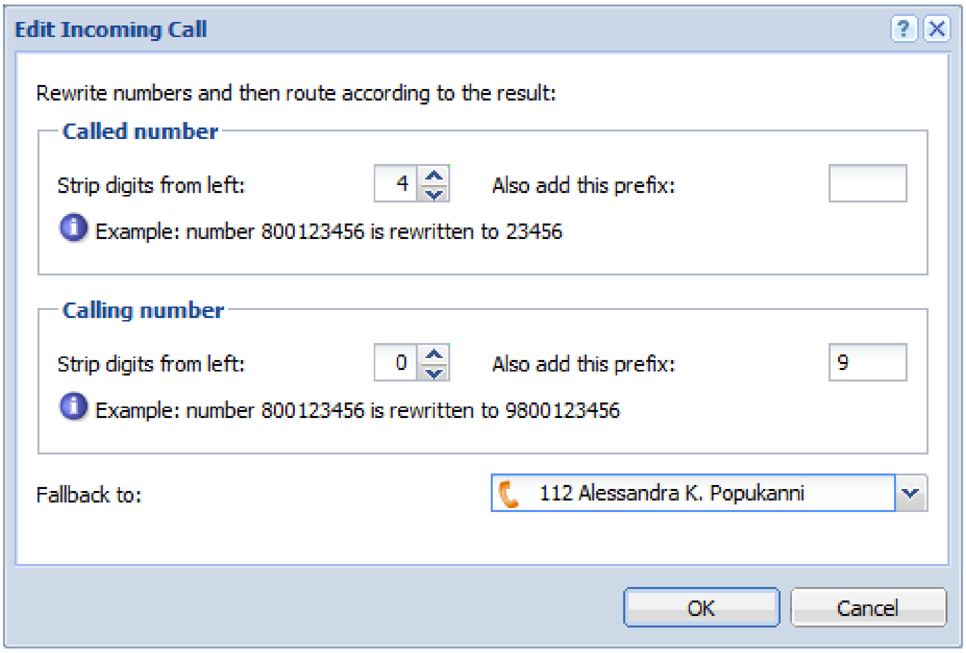

Figure 6.6 Rule for interface provider1

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).

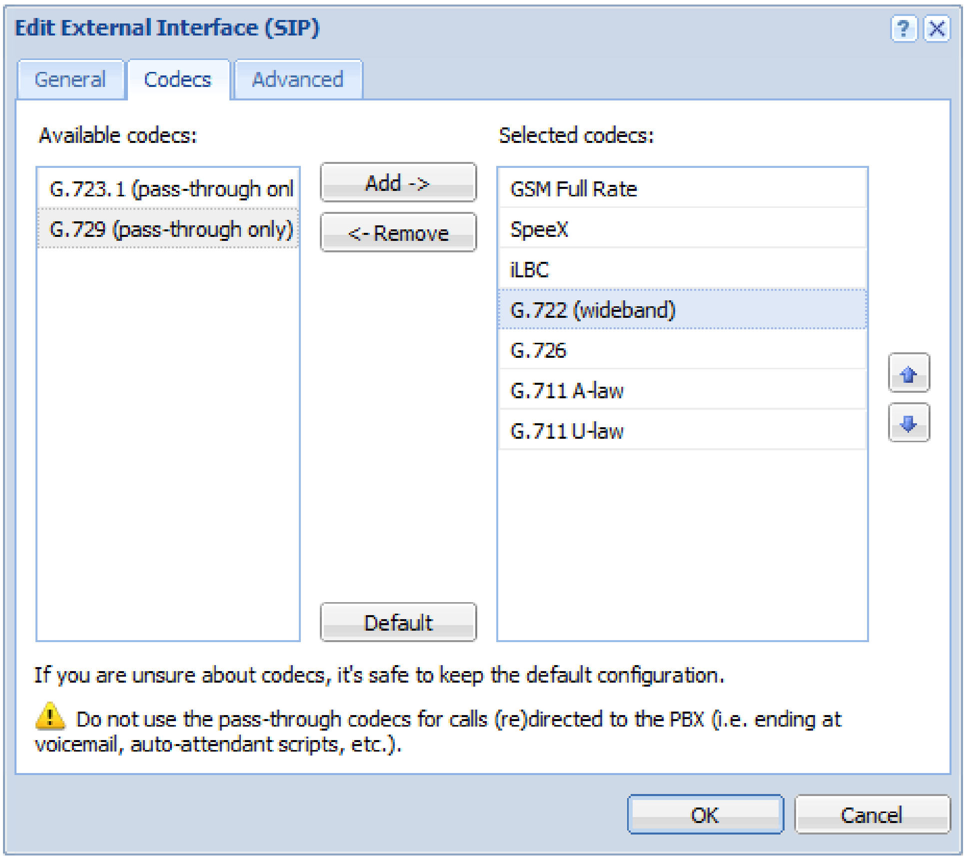

Figure 6.7 Interface for incoming calls → Codecs tab

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).

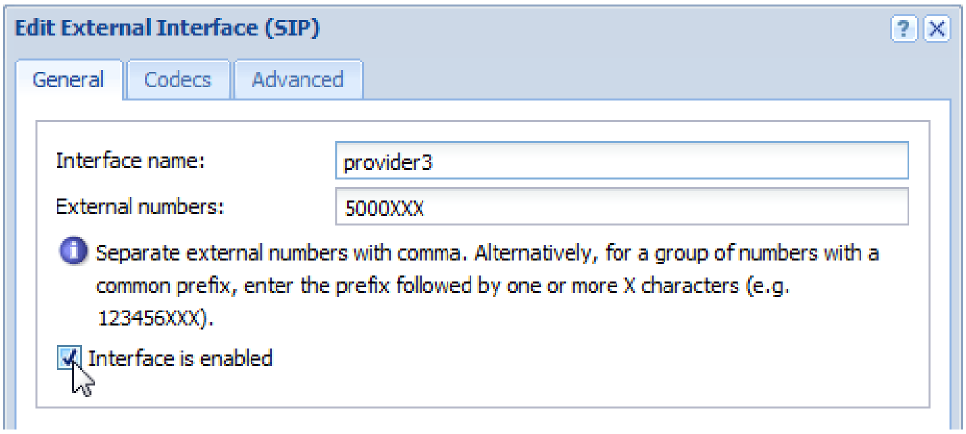

Figure 6.8 Block interface

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 and deploy a PRI, BRI or FXO card. 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 connection. The interface needs to be configured for both incoming and outgoing 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 — 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.
- FXO card — has 4 ports. Each port can operate one concurrent call.

7.1 Configuring PRI/BRI/FXO 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 to know:

- telephone number or numbers form your telephone provider,
- (only PRI/BRI) 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 available 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 standard 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).

   If the FXO 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 must not contain spaces, national and special characters and must be unique.

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 operator 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 PBX of your telephone provider.

4. Click on *Next*.

5. (Only PRI and BRI) Select the PBX type in the dialog:

   - 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 operator who will direct all external calls made to 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. (Only PRI and BRI) Select the PBX type in the dialog:
    - 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 an 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 which 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. (Only PRI and BRI) Select the PBX type in the dialog:
    - 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. Finally, 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/FXO interface for communication with another PBX

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

1. In the administration 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 must not 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 other server uses extensions 3XX), all 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. Finally, create a rewriting rule for correct mapping of numbers to internal user extensions. See section 7.3 for more details.

7.3 How to configure 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. Analogue 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 a shortened form (usually last 4 digits) which are sufficient for recognition of the correct extension. Similarly, the provider may also require whole numbers or numbers in a shortened form (usually last 4 digits). Request this information from your provider before you start configuring the interface.

See the following example of rewriting rules:

- Company acquired 100 phone numbers from their telephone provider (an interval 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 interval 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 Kerio Operator.
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 arise 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 callback rule. To achieve this, add a prefix for calling to external network (otherwise, callback will fail at the outgoing call interface).

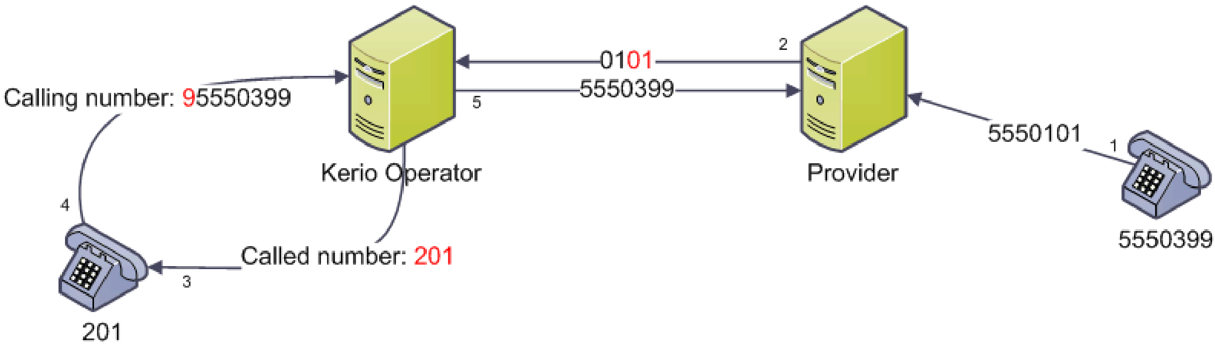

Figure 7.1 Incoming and answer call (read from right to left)

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

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

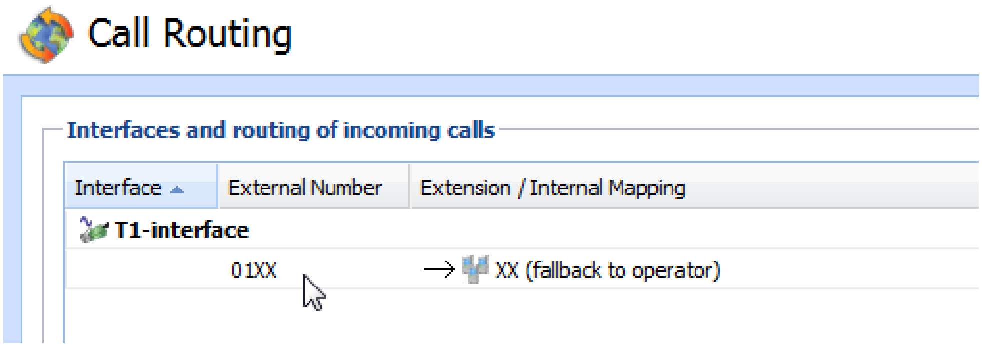

Figure 7.2 Rule for standard telephone interface T1

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 provides the final format of the internal extension (2XX).

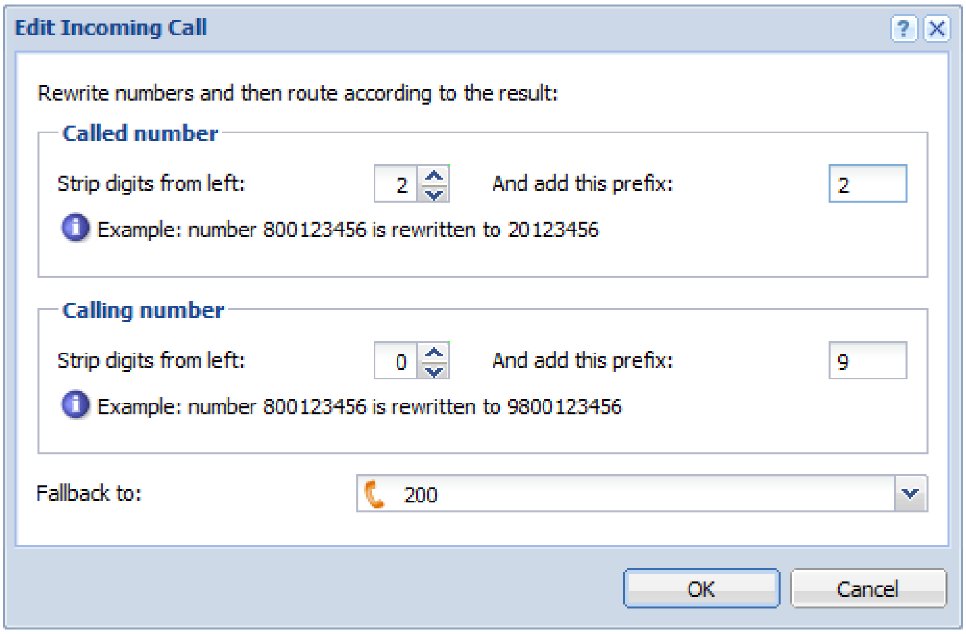

Figure 7.3 Rule for standard telephone interface T1

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 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 in our case is number 9. Final format of the number 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.

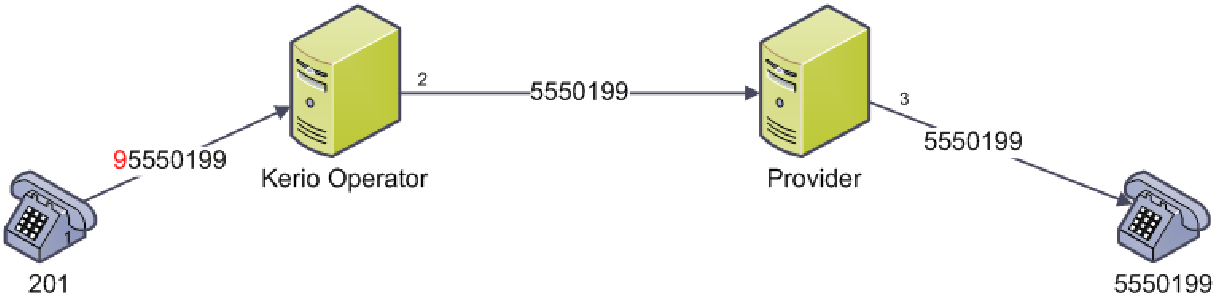

Figure 7.4 Scheme describing how to adapt called number

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 achieve the above mentioned interface behavior:

1. In Kerio Operator Administration in section *Call Routing*, double-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; go to the *Rewrite Numbers* tab.

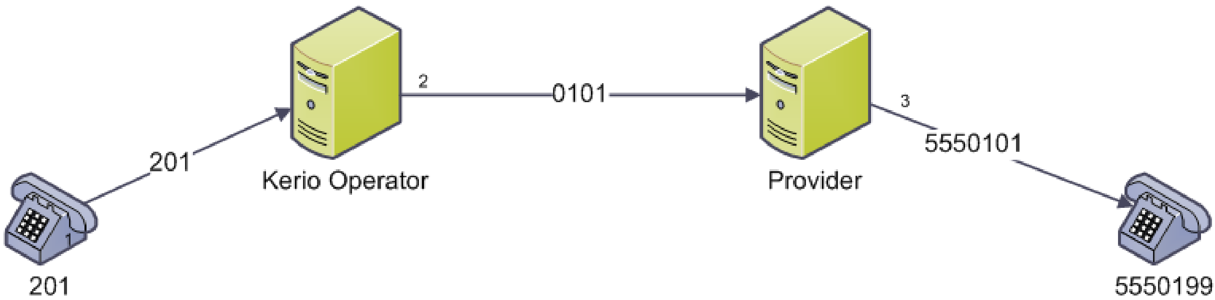

Figure 7.5 Scheme describing how to adapt calling number

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).

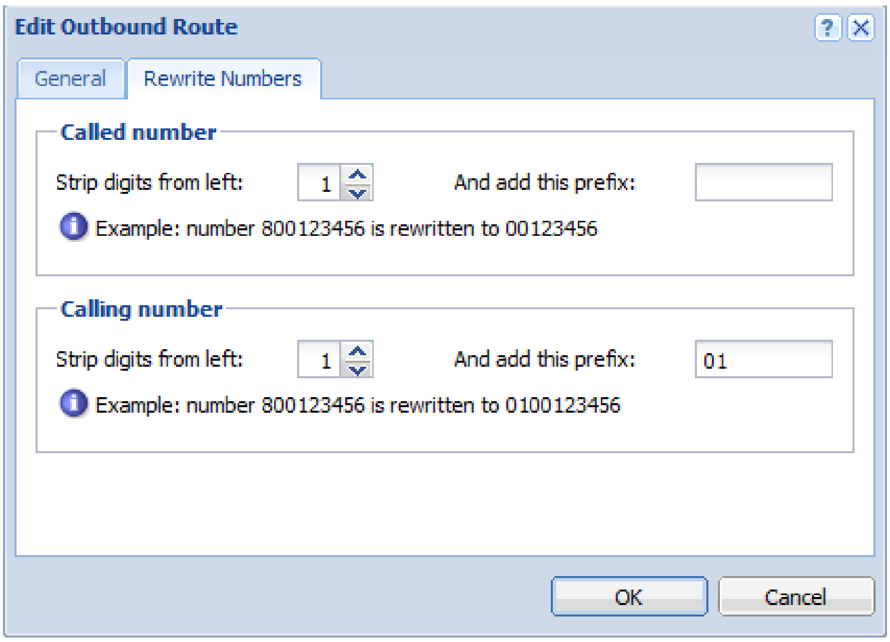

Figure 7.6 Outbound route

7.4 Overlap dialing

Some telephone providers 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 the administration interface, open the *Call Routing* section.
2. Double-click the interface to open dialog *Configure PRI/BRI/FXO 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. Enter *SIP password*. Please follow the parameters for creating secure passwords. Attackers can easily guess simple passwords, call via your PBX and cause significant financial losses for your company.

   Note: After saving and reopening the dialog, icon with keys is displayed next to the password. Click on it to see the SIP password.

5. 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.
- 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 network 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.

Note: Some registrars (VoIP service providers do not allow hiding phone numbers). If you are connected through such registrar, the settings will not work. For more information, see section 6.1.

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*),
- to his company cell phone (to be available in case the server is down),
- we disable redirecting to voicemail because his boss hates voicemail.

Configure the redirecting as follows:

1. Go to section *Users* and double-click the IT administrator account from the example.
2. In edit user dialog, go to the *Ringing Rules* tab.
3. Select the *Forward to* option and enter the cell phone number in appropriate format. This means a format which is required by the VoIP service provider. Also add the prefix for outbound calls (you can set the prefix in section *Call Routing* — 6).
4. Disable *Fallback to voicemail*.
5. Save the settings.

Note: Users can also use the Kerio MyPhone interface to forward their calls. Therefore make sure that you do not overwrite their own settings.

With every forwarded call, the auto attendant script informs the caller that the PBX is trying to find the callee. If you wish to disable this information or change to music while waiting, configure option *While forwarding a call* in section *Configuration* → *Advanced Options* → *General*.

8.4 Changing Access Rights

Kerio Operator uses the following system access roles:

- user — has rights 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 Accounts

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

If users are mapped from Active Directory and you disable users in the directory service, they will also be disabled in Kerio Operator.

If users are mapped from Open Directory and you disable users in the directory service, they will stay enabled in Kerio Operator.

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 account until you enable it again. All their phone extensions will be deactivated. Deactivated phone extensions stay active in the system but they do not accept incoming or outgoing calls.

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 Configuring Extensions

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 a way 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 27.1).
5. (Optional) You can allow multiple registration for an extension and generate other necessary usernames. This is necessary if a user uses more than one manually configured phone (especially softphones on computers or SIP phones on mobile phones). For details about this function, go to chapter 16).
6. 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).

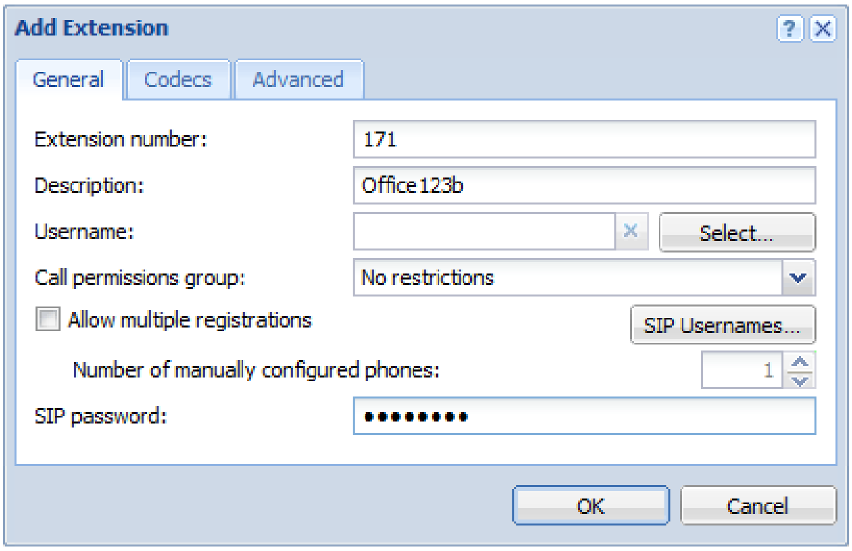

Figure 9.1 Adding new extension

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.

For the list of the phones, refer to the Kerio Operator product pages.

Note: 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:
Use of phone provisioning is not always suitable. If Kerio Operator is located and runs in the Internet, for security reasons we do not recommend to use automatic phone provisioning.

Phone provisioning requires:

- configuring the PBX
- 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 phone provisioning works:

- The telephone boots in the network and sends a DHCP request for an IP address.
- DHCP server accepts the request, assigns an IP address and sends it back in a DHCP reply. Besides the IP address, the message also contains TFTP (Trivial File Transfer Protocol) server address — Kerio Operator, in our case.
- 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 for the phone;
    - if it is not new, Kerio Operator finds the extension which the phone has used.

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

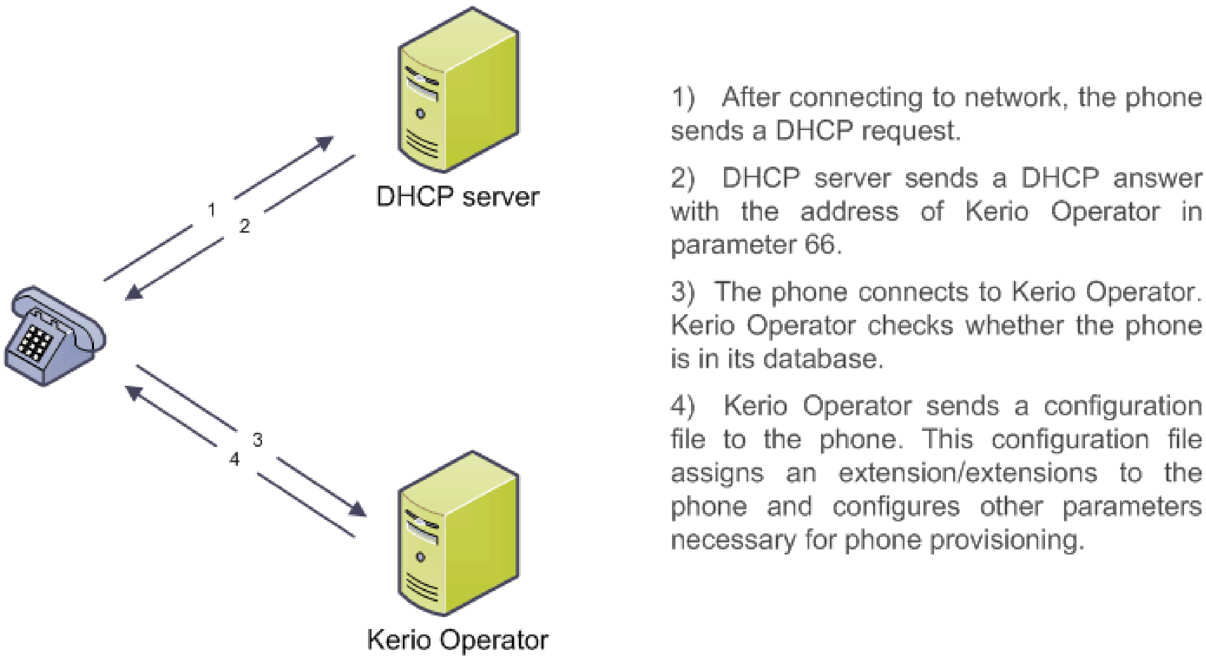

Figure 10.1 Automatic HW phone provisioning

- 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 be used as a stating number for 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 was 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.

> ***Warning:***
> This option is checked by default. If you uncheck it, you cannot use automatic remote phone restart — you will have to restart phones manually if needed.

4. In the *Password for phones* field, you can change the SIP password for all provisioned phones. You can use any password, however, we recommend to follow secure password policy. 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.[2]

   Clicking the icon with keys displays the current SIP password.

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 documentation 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:

1. In section *Configuration* → *Provisioned Phones*, click on the *Add manually* button.
2. This opens 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).

[2] The password is saved in the configuration file which is sent to the phone upon the first connection to the network and the phone will use this password to authenticate at Kerio Operator.

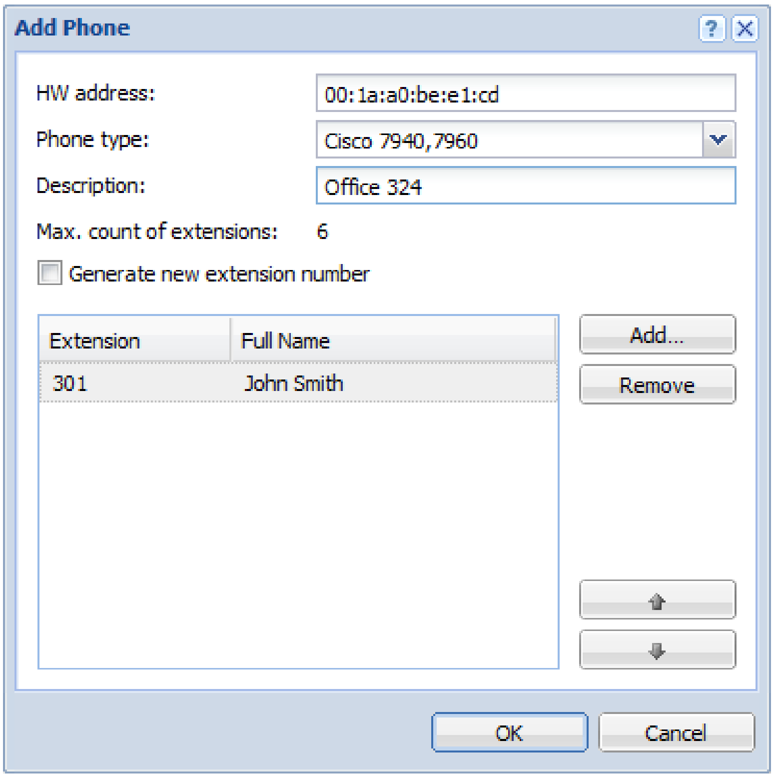

Figure 10.2 Connecting a phone manually

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 divided by a semicolon.

The file may look as follows:

```
00:1a:a0:be:1e:cd;Cisco;7940;111;112
00:1b:b0:cd:e1:ca;Cisco;7960;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 wish 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. Now, we can remove the phone in the *Configuration* → *Provisioned Phones* section by click the *Remove* button.

10.5 Restarting provisioned phones

When you change phone provisioning configuration, all the phones need to be restarted (for example, when you create a 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 Firmware

Kerio Operator allows easy installation of phone firmware 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 firmware* dialog, select the appropriate phone.

5. Click *OK*. to confirm changes.

Chapter 11

Mapping Users from Directory Service

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

- user accounts are configured and managed in the directory service which reduces administrative complexity and error,
- users can use the same username and password for login to their domain and to *Kerio MyPhone*.

Warning:

- Mapping is one-way only, data are synchronized from directory service to Kerio Operator. Adding a new user in Kerio Operator creates a local account — it will not be duplicated into the directory service database.
- When creating user accounts in a directory service, ASCII must be used to specify usernames. If the username includes special characters or symbols, user may not be able to login to Kerio MyPhone or the administration interface.
- If you disable users in Active Directory, they are also disabled in Kerio Operator (they will not be able to log in to Kerio MyPhone, make or receive calls with their extensions).
- If you disable users in Open Directory, they stay enabled in Kerio Operator.

Phone extensions can be managed in a directory service (if available) or locally in Kerio Operator. Select the most convenient option.

To map users from a directory service:

- connect to directory service in section *Configuration* → *Advanced Options* → *Directory Service*.
- activate users in section *Configuration* → *Users*.

11.1 Connecting to Directory Service

In the administration interface, go to *Configuration* → *Advanced Options* → *Directory Service*.

1. Check the *Map user accounts from a directory service* option and select your directory service type.
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 use 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 *Apple Open Directory* Administrator, not just a local administrator on the *Apple Open Directory* 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.

11.2 Activating Users

Once the mapping is set, select individual users and map them to the PBX. This is how to map users:

1. Go to *Configuration* → *Users*.

2. Click on *Add* → *Add from Directory Service*.

3. In the dialog, select all users you wish to map (you can also add users later) and click *Next*.

4. If users in the directory service have phone extensions assigned, you can either keep them or disable them. If you disable them, you have to assign new extensions. You can do it, for example, while changing your dial plan.

   Note: Only extensions in attributes `telephoneNumber` (Active Directory, Open Directory) and `otherTelephone` (Active Directory) can be mapped (are displayed). If you create special attributes in a directory service for your phone numbers, you will not be able to map such extensions.

5. Click on *Finish*. Activated users are displayed in section *Configuration* → *Users*.

Chapter 12
Dial Plan

The dial plan contains 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 described 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 this warning, phones will be restarted at the time you selected in the dialog. You can restart the phones later manually in section *Provisioned Phones*. To restart the phones, click on the *Advanced* → *Restart all phones* button.

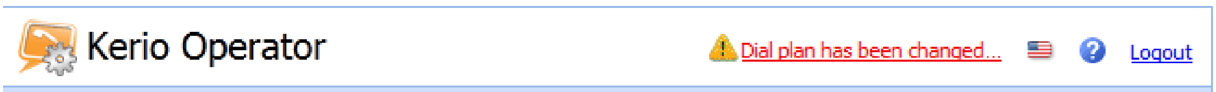

Figure 12.1 Changing the Dial Plan

Chapter 13

Telephone Conferences

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

Telephone conferences allow participation both of users defined in Kerio Operator and external participants. To join a particular conference it is only necessary to dial conference number and its access code if desired.

13.1 Creating New Conference

1. Go to section *Configuration* → *Dial Plan* and make sure that the line you have selected for the conference is not used.
2. Add a new conference in section *Configuration* → *Conferences*.
3. Click on *Add*. This opens the *Add conference* dialog.
4. Enter the conference extension and its description.
5. Optionally, you can limit the number of participants. Too many participants increase demands on the server and affect its performance.
6. Each conference can be protected by a PIN required from all participants upon entering the conference. If you wish to secure a conference, set a PIN and deliver it to the members.

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 terminate the call.

13.3 Viewing Active Conferences

All current conferences can be viewed under *Status* → *Conferences*. The window displays two tables. Each line in the first table displays one conference. The second table displays information about individual conferences. Just select a conference and the details in the bottom table are updated.

Chapter 14

Call Queues

Call queue is a tool which enables your customers or other callers 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*.

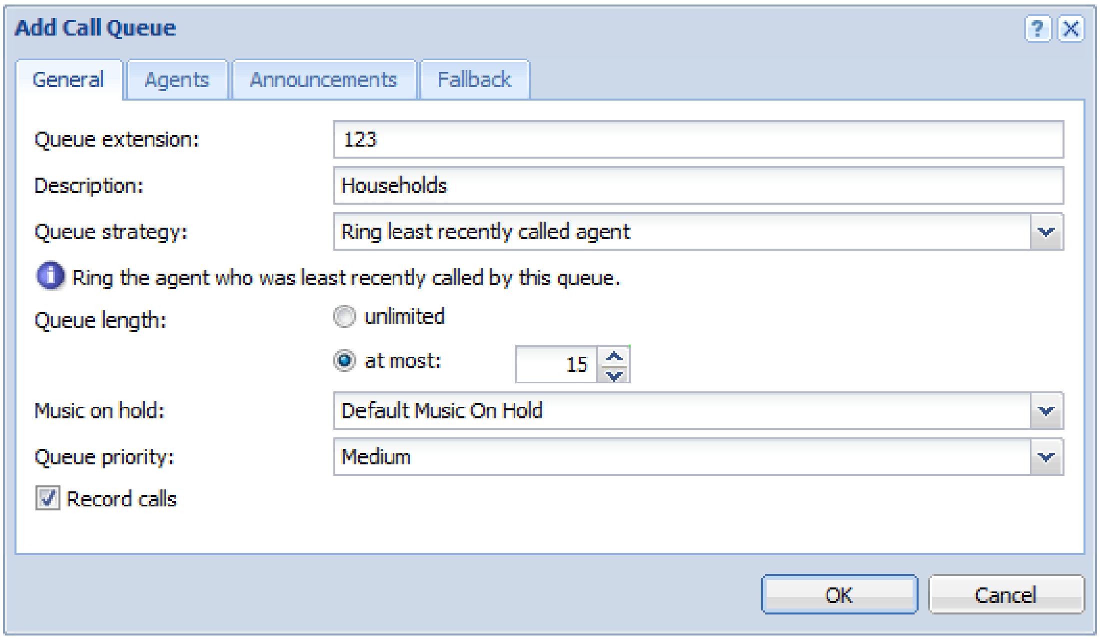

Figure 14.1 Call Queue — General tab

1. On the *General* tab (see figure 14.1), fill in an extension 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 14.3) are called repeatedly in the same order.

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

- Ring least recently called agent — the system selects the agents who have 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.
- Ring in order — use this option only if you have solely permanently assigned agents on tab *Agents*. Put the permanently assigned agents in order; the agents will then be selected in the same order. This strategy is for companies where all calls are answered by a receptionist. In case the receptionist is not answering, the call is directed to next agent in order (for example, an administration assistant).

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 their waiting time is. 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 it to Kerio Operator (see chapter 28).

14.2 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. The option for recording calls is on the *General* tab.
3. Check the *Record calls* option.

List of recorded calls

Section *Status* → *Recorded Calls* displays all calls recorded from call queues. This section displays a table where each recorded call occupies one row. Select a call to listen to it, download it to your computer or remove it.

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 opens 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 are deleted.

14.3 Agents

Agents are telephone operators who attend call queue and answer customer demands. 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).

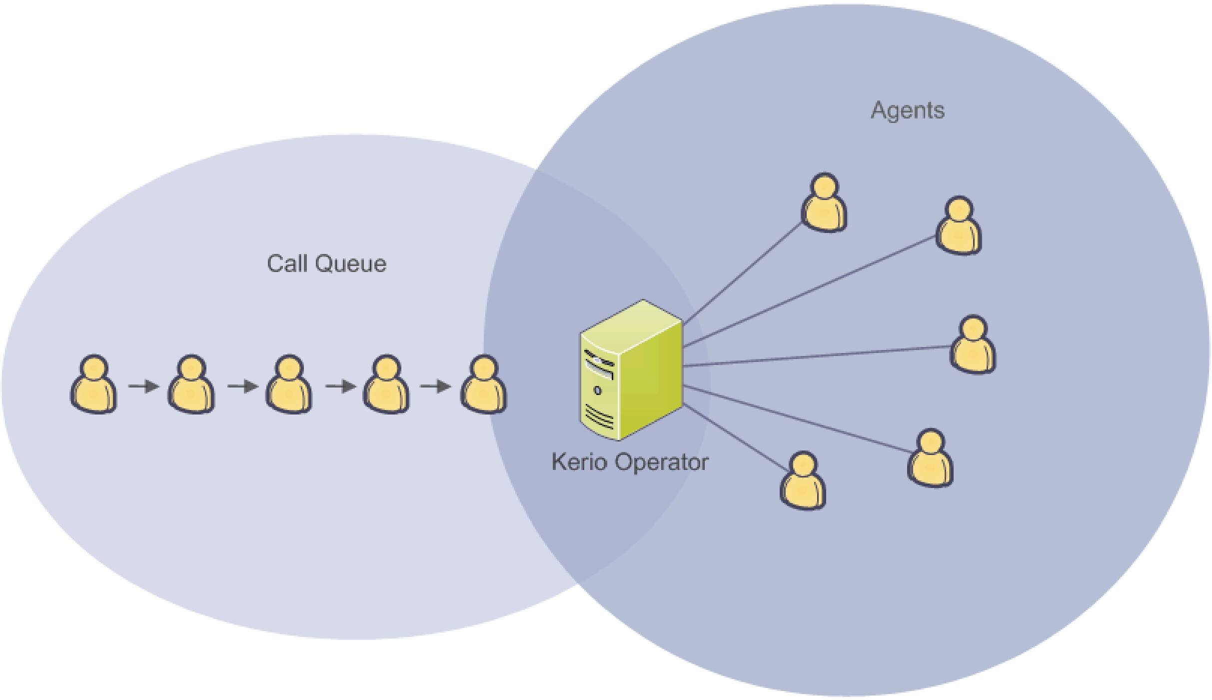

Figure 14.2 Call queue

Agent login and logout

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

- Dynamic login/logout — each agent has their own phone. 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 options above. Some agents are permanently assigned and others login dynamically. This is convenient during the peak-hour shift. The queue is then attended by more agents than in other shifts.

Apply settings as described below:

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

   Set static or dynamic agent login. If you check the *Allow dynamic agent login/logout*, enter codes for the queue's login and logout. Make sure the codes are different from the extension numbers. Permanent agents can be added in table *Permanently assigned agents*.
3. Regardless of the queue strategy, you may set time when no call will be connected to the agent. This enables the agent to process the call. If your agents need to fill in a record after each call, set the appropriate time in the *Give agents this wrap-up time after each call* menu.
4. The last settings are for situations when an agent is logged into the queue, it is their turn but they are not answering the phone. For such cases, set a time limit after which the queue will be directed to the next agent in line (according to the queue strategy).

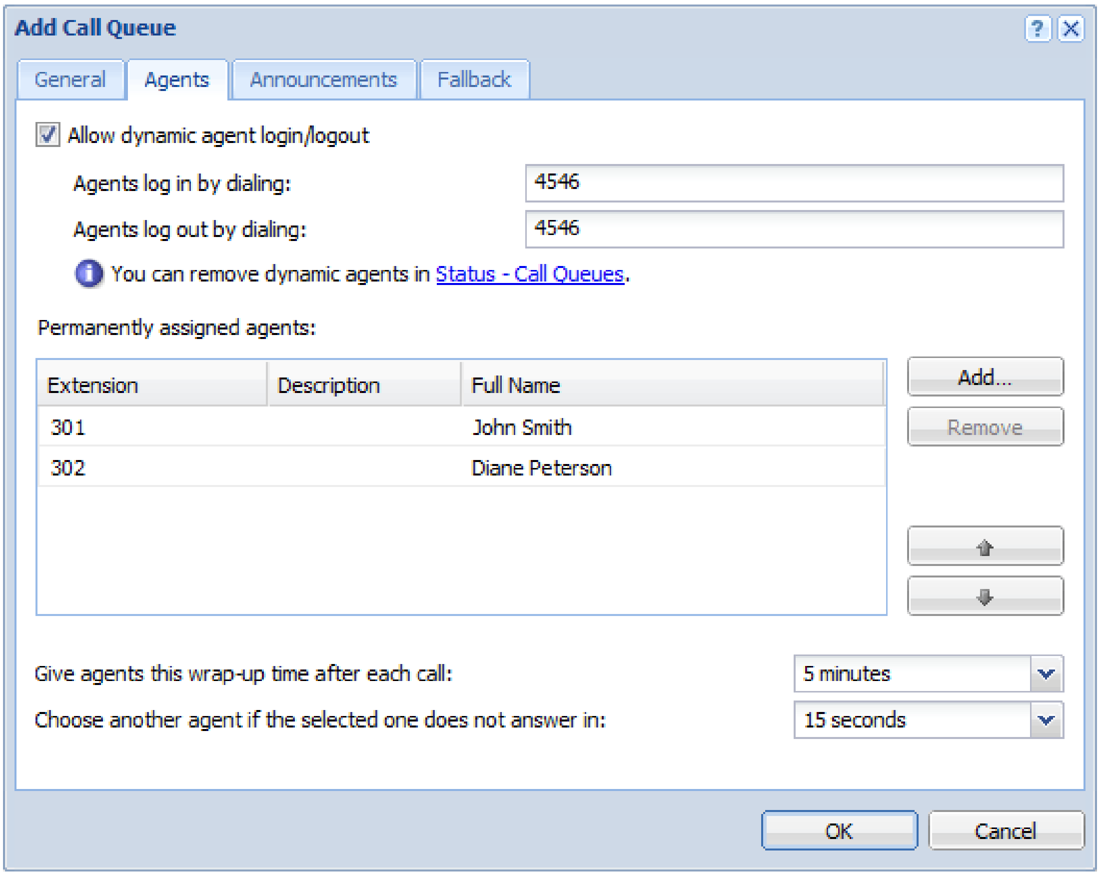

Figure 14.3 Call Queue — Agents tab

Operating multiple queues at once

Agents do not have 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.

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

Upload new audio record 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*.

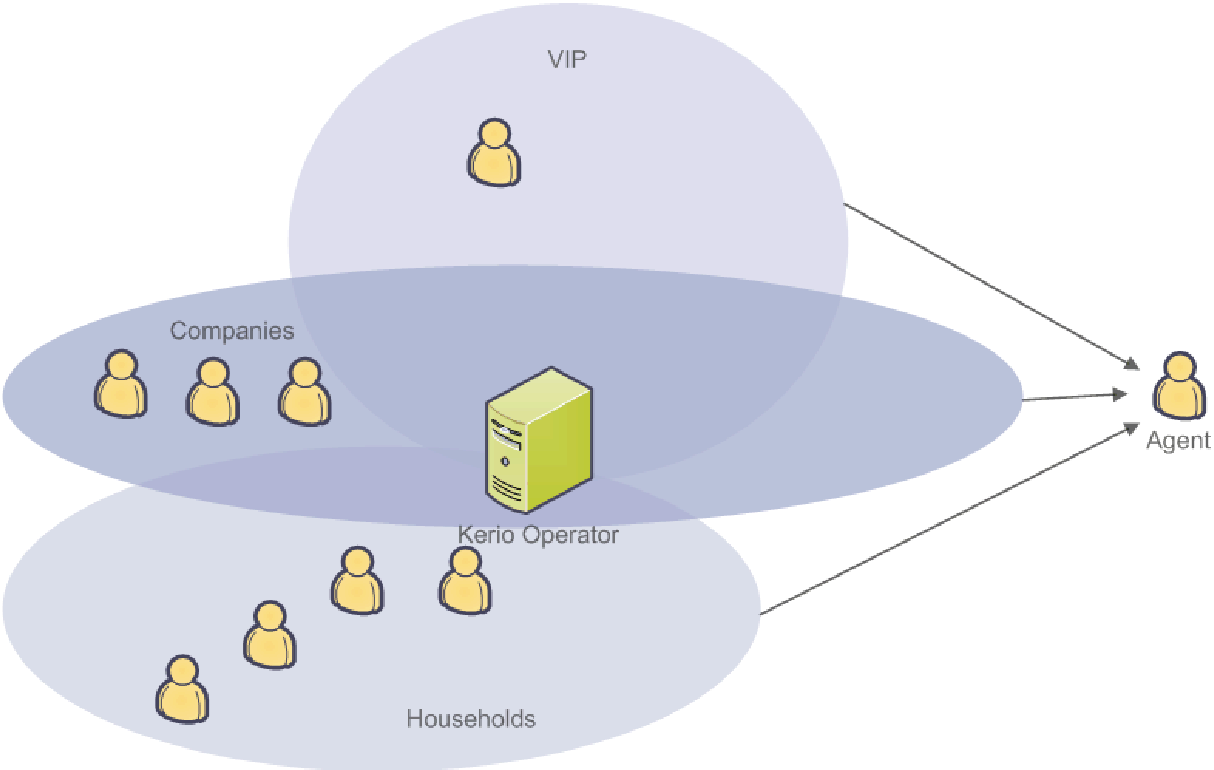

Figure 14.4 Operating multiple queues at once

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 *General* and set the desired priority.
4. Repeat the configuration for other queues.

14.4 Announcements for Callers in a Queue

Customer waiting in a call queue can receive the following information while waiting:

- Greeting message.
- Any custom announcement (for example promotional announcement or an apology for waiting) which can be periodically repeated.
- Position of the customer in the queue, possibly also estimated hold time (Kerio Operator is able to count the average waiting time of the previous customers). You can also set the language of these announcements.
- Announcement that the queue is full and the customer will not be accepted in the queue.
- Announcement that no agent is operating the queue.

Apply these settings by using the following instructions:

1. Prepare sound files in WAV or GSM where individual announcements will be recorded. More information on how to easily record announcements can be found in 17.2.
2. Open the *Configuration → Call Queues* section and select the queue.
3. In the displayed dialog, go to tab *Announcements*. Focus on section *Customers*.
4. First, set the greeting message. Click on *Select* in the *Welcome announcement* row and upload the particular audio file to the PBX or select it directly.
5. Now set periodicity. In *Play the following announcement each*, select a periodicity. Then click on *Select* and upload the particular audio file to the PBX or select it directly.
6. Select the repeat cycle for the position in queue announcement. If you wish your customer to know the estimated waiting time in the queue, check the *Include estimated hold time when entering the queue*. You can also select the announcement language.
7. Set the announcement that the queue is full (only if you restrict the queue length on tab *General*).
8. You can also record and enable the announcement that no agent operates the queue.

14.5 Directing calls when agents are unavailable

These settings the following situations:

- At least one agent is logged in to the queue but no one is answering (example: they forgot to log out before leaving the office).
- No agent is logged in to the queue (example: the agents are off the clock).

Configure the first example as follows:

1. Open the *Configuration* → *Call Queues* section and select the queue.
2. In the displayed dialog, go to tab *Fallback*.
3. Check *Fallback to another extension* and enter the extension to which the call in the queue will be directed (to an operator or chief agent). This solves the situation when agents are logged into the queue but no one is answering the calls.
4. Set the time period after which call will be directed to another extension.

Now, configure the second example as follows:

1. Check *Callers cannot join the queue* (otherwise, they would wait in the queue for the next agent login).
2. Check *Terminate calls that are already waiting* (otherwise, they would wait in the queue for the next agent login).

14.6 Viewing Call Queues

All active call queues and their parameters can be observed in section *Status* → *Call queues*. The window displays three tables. Each line in the first table displays one call queue.

The other tables display agents and callers in a queue. Just select a queue and the details in table *Agents* and *Callers* are updated.

You can also reset the call queue statistics to start from zero. Use the *Reset 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 employees 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 no one from the ringing group answers the phone, check the *Fall back to another extension when the group is not responding*.

Chapter 16

Multiple Registration of an Extension

Multiple registration of an extension gives the possibility to register one extension to multiple phones. You must generate and use several special strings (usually called User ID or Auth ID). One for each phone. This prevents stealing of the username when two phones are used simultaneously (for example, SIP client on your mobile phone and another on your computer). Provisioned phones do this automatically. Manually configured phones have to be assigned various User IDs.

This is best shown on the following example:

User Winston Smith with username `wsmith` form the Sales department has extension 124. He works partly form home. He uses the following to communicate:

1. He has an automatically provisioned phone Cisco 7940 in his office.
2. He has X-Lite softphone on his home computer.
3. Occasionally, when connected via WiFi, he uses a SIP client on his mobile phone.

Solution:

1. Go to Kerio Operator Administration to section *Configuration* → *Extensions*.
2. Double-click on the John Smith's extension 124. This opens the *Edit extension* dialog.
3. Check the *Allow multiple registrations* and set the *Number of manually configured phones* to 2 (for X-Lite and SIP client on your mobile phone).
4. Click on *SIP Usernames* and note the strings (with letter "u" at the end).
5. Save the settings.
6. In the SIP client and softphone configurations, enter the newly generated strings as User IDs.

Chapter 17

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 receive information directly or they will be connected, as soon as possible, to an extension with agent ready to help them.

Auto Attendant Scripts allow to:

- Quickly connect the caller to desired extension, to desired department.
- Answer frequently asked questions — customers get necessary information (for example, address or opening hours) without waiting.
- Raise the productivity of your employees — it reduces the time your employees spend connecting calls.
- Availability to callers during 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 behavior. It can:

- connect to an extension or voicemail,
- play an announcement,
- navigate through menus and submenus.

Menus can be recorded in various formats. Kerio Operator supports the following formats (see table 17.1):

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

Table 17.1 Kerio Operator — supported audio formats

17.1 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,
- contains a voice menu with the following 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 talk 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.com*. The receptionist will connect 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*:

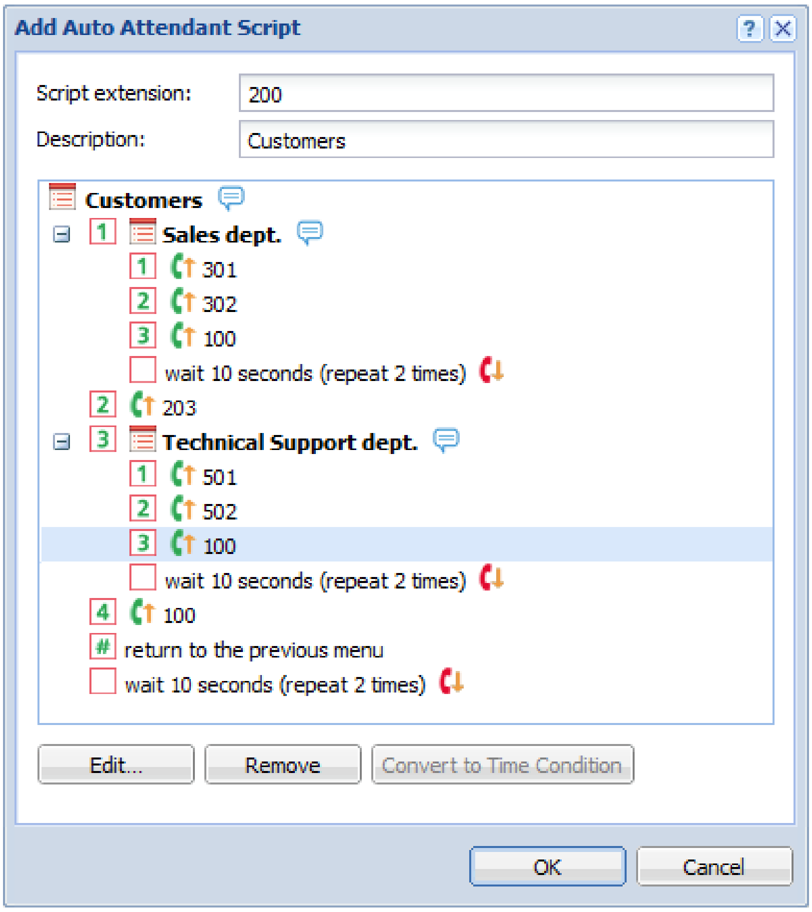

Figure 17.1 Auto Attendant Scripts

1. Click on *Add* and enter the *Script extension* (extension 200 in our example) and some description (see figure 17.1).

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

3. In the *Announcement* field, select the recording for the main script. The *Select* button offers existing recordings or you can upload your own announcement to the PBX.

4. Set *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 action. This means that if the announcement is played twice and the customer does not make any selection within 10 seconds, the call will be terminated.

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 *Go to submenu*. We need 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 17.2.

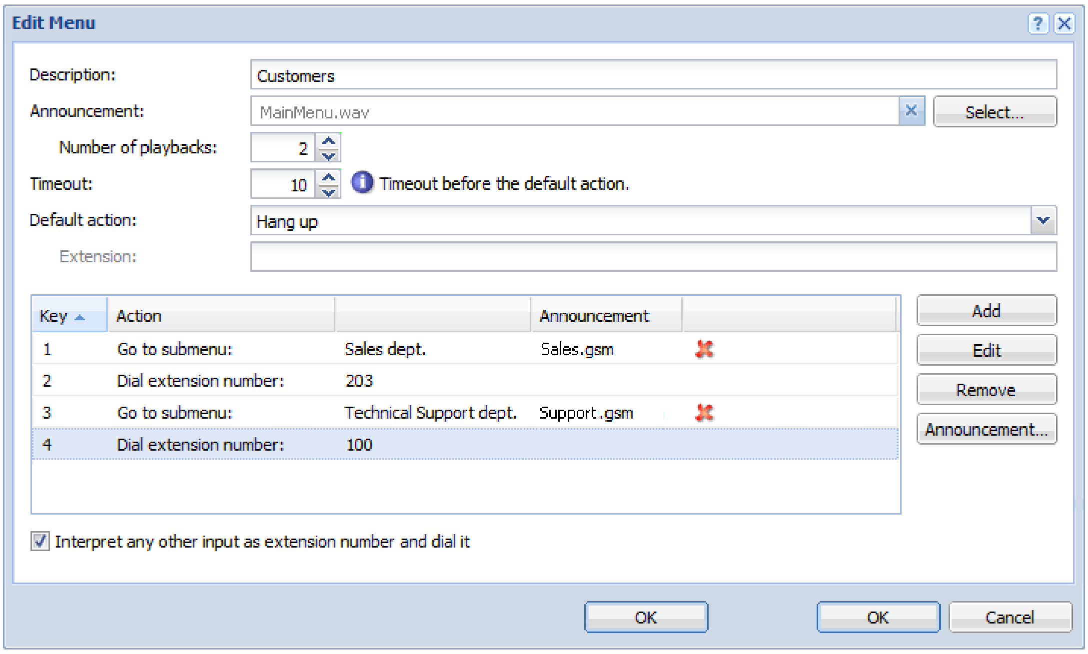

Figure 17.2 Editing main menu

7. Check the *Interpret any other input as extension number and dial it* option. This option allows to specify a direct extension while the auto attendant script is running.

8. Confirm the settings and return to the *Add Auto Attendant Script* dialog which is now similar to the one in figure 17.1.

9. Click on the *Sales Dept.* menu. Again, the *Edit menu* dialog is opened but now the menu is for the Sales dept. Proceed similarly as with the main menu. The final menu will look as the one in figure 17.3.

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

11. Now the script is complete.

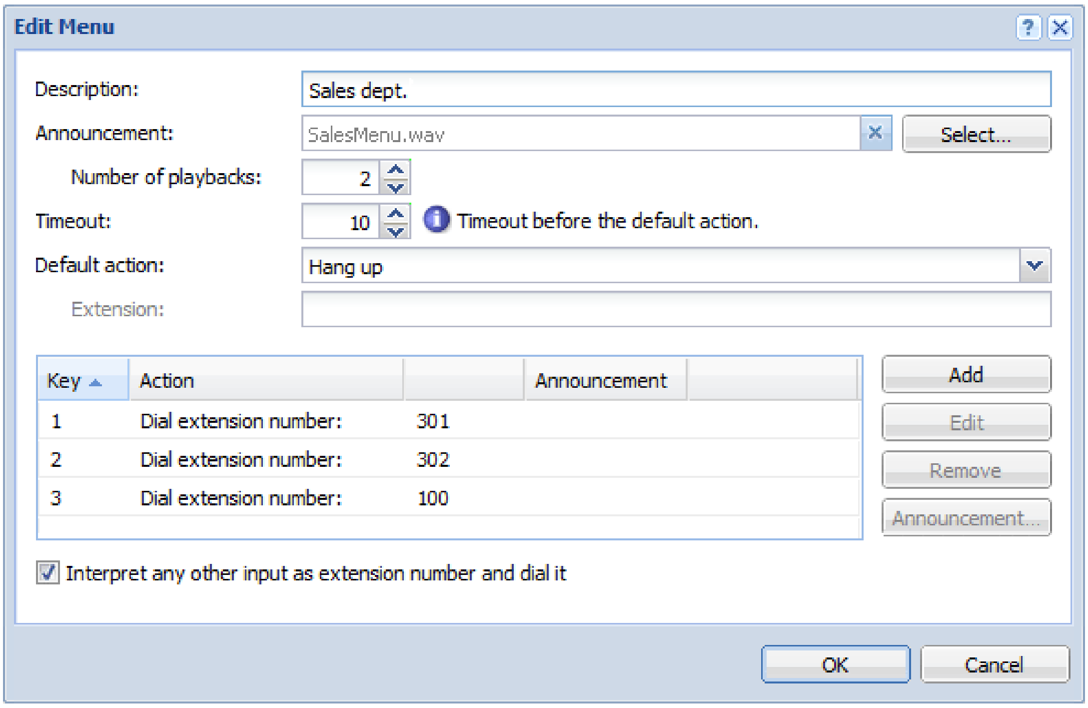

Figure 17.3 Submenu edit

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 29). 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 Attendant 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 17.1).

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 one is played 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 17.4).

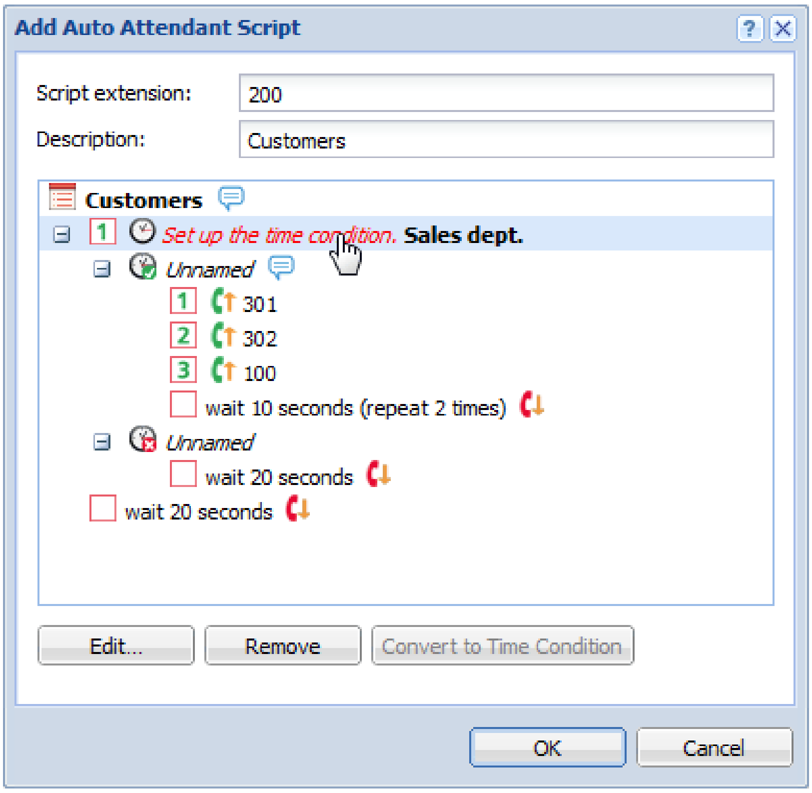

Figure 17.4 Setting the time condition

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 you can 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 17.5.

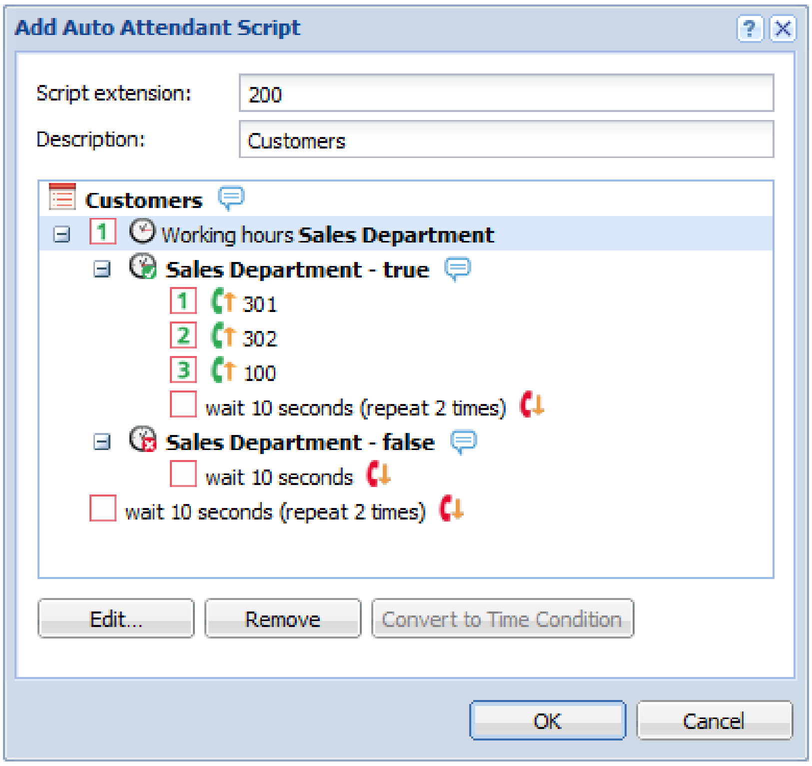

Figure 17.5 Time condition applied in the script

17.2 Creating a voice recording

This chapter shows how to create a recording for an auto attendant script easily, fast and in sufficient quality.

1. Prepare texts.

2. Pick up the handset of your phone which is connected to Kerio Operator.

3. Dial the *Record audio* (extension 86).

Note: If this service in unavailable, go to *Configuration* → *PBX Services* in the administration interface. The service may be disabled or may use another extension.

4. Say individual voice recordings into the headset.

5. You can listen to the recordings are in section *Configuration* → *Auto Attendant Scripts* (the *Audio File Library* button is in the right bottom corner).

Chapter 18

PBX Services

Kerio Operator has special phone extensions which run the following services:

- *Directed call pickup* — this service enables the receptionist or personal assistants to answer calls for other extension. Press the asterisk button twice ("**") and dial the extension number. Imagine the following situation:

    - the managing director uses extension 101
    - the financial director uses 102
    - they share a personal assistant

    If the assistant's phone shows information that somebody is calling the managing director during his meeting with the financial director, she can accept the call by dialing **101. Next call is for the financial director and the assistant can also accept this call. This time she dials **102.

    As you can see, by dialing the call pickup code, you can answer a call for any extension of the PBX.

- *Call pickup* — this service enables creating and using call pickup in groups (see section 26).

- *Echo* — this option helps you monitor whether phones are correctly connected and what is the sound delay. Speak to the phone after hearing the automated message. If done correctly, your message is recorded and played back.

- *Music* — music plays upon dialing the extension.

- *Current time* — auto attendant tells the current date and time.

- *Dial by extension* — auto attendant invites the user to enter the extension which the operator will dial.

- *Dial by name* — user enters first several letter of the callee's surname and system searches the address (created in *Kerio Operator*) and dials the extension.

- *Record audio* — *Kerio Operator* starts recording. *Kerio Operator* enables you to easily record recordings for auto attendant scripts in excellent quality.

Warning:
If you wish to you any service, tick the box next to this service. Extensions offering the services are disabled by default.

Chapter 19

Speed Dial List

In Kerio Operator, you can create a speed dial list. They are shortcut numbers of called numbers. Imagine a taxi dispatcher. They constantly call employees' mobile phones. Dialing whole phone numbers would take long. Therefore, we create the following list in Kerio Operator — see table 19.1.

Last Name, First Name	Phone Number (including the prefix for outbound calls)	Speed Dial
Conrad, Paul	0111234567	11
Darwin, Diane	0111234566	12
Davidson, Irene	0111234565	13
Fogg, John	0111234564	14
Newman, Daniel	0111234563	15
Peterson, Winston	0111234562	16
Skolowski, Luke	0111234561	17
Smith, John	0111234568	18
Smith, William	0111234569	19
Wayne, Derek	0111234570	20

Table 19.1 List of taxi drivers

Note: Speed dial behaves like a standard phone extension. It may have any number of digits and may be used to dial an external number.

19.1 Creating a Speed Dial List

Before you begin creating speed dial, select a numerical range you will use. Speed dial must be different from extensions. Generally, it is convenient to create speed dial so that they will not coincide with your dial plan in future.

1. Open the *Configuration* → *Speed Dial* section.
2. Click on *Add*.
3. This opens a dialog where a new speed dial can be added. Enter a speed dial in the *Speed dial extension* field.

Note: Speed dial must not coincide with an existing phone extension, otherwise you will not be able to create it. You can check created extensions in section *Dial Plan*.

4. In *Description*, enter at least the name of the callee or you may not know who was assigned the speed dial.
5. In *Dial number*, enter the callee's phone number including the prefix for outbound calls.
6. Save the settings.

Chapter 20

Voicemail

Voicemail works similarly as a hardware message recorder but messages are stored on the server and they can be forwarded to user email boxes.

Voicemail allows:

- forwarding calls to voicemail if the user is unavailable,
- forwarding calls to voicemail if the user is busy,
- accessing user voicemail directly (for more info, see section 20.2),
- sending voice messages to your email box.

If you also use Kerio Connect, you can configure Kerio Operator and Kerio Connect to cooperate together. Kerio Connect and Kerio Operator synchronize the flag which identifies whether the message has been played.

20.1 Voicemail Settings

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

1. Configure the greeting message for callers who are redirected to the callee's voicemail:

   Instructions inform the callers what they should do next: "Leave a message after the beep".

   Message informs the callers that the callee is unavailable.

2. The *Voicemail access extension* field includes extension number — once the users dial this extension and enter their PIN number, they are connected to their voicemail and can play their voicemail messages. If you do not like the extension

3. Set each user their PIN on the *General* tab in section *Configuration* → *Users* (see section 9.1).

Additional voicemail settings can be configured in section *Configuration* → *Users*:

1. In account settings on tab *Extensions*, assign users their PIN (see section 9.1). Users use the PIN number for authentication to access the voicemail via their phones.

2. Each user can have different settings for voicemail when they are unavailable. Change the settings on tab *Ringing Rules*. Automatic redirect to voicemail when unavailable or busy

is enabled by default. You can adjust the settings in the administration interface or users can do it themselves in Kerio MyPhone.

20.2 Direct access to user voicemail

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

To configure 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.

20.3 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.

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

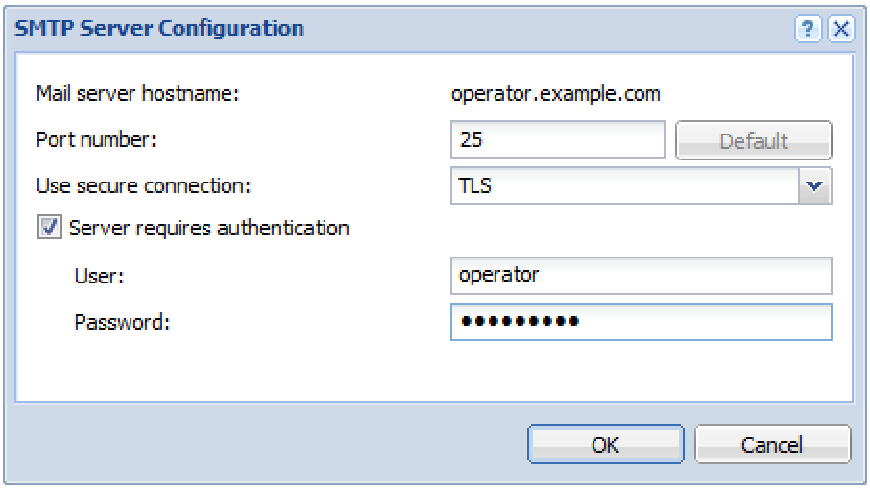

Figure 20.1 SMTP configuration for sending voicemail messages

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* → *Email tab* and check the *Send each message 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 SMTP server requires authentication, check *Server requires authentication*. Use the username and password for the account you created on your mail server in step 1 (see figure 20.1).

7. Click OK to confirm settings.

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

To send voicemail messages to email inboxes of the users, you need to set their email addresses in the Kerio Operator Administration in section *Configuration → Users*.

Note: If the users' INBOXes are unavailable (the mailserver is down), the user accounts are disconnected from voicemail and try to reconnect every 5 minutes. Each attempt to connect is recorded in logs.

Integrate with Kerio Connect

Integration with Kerio Connect allows synchronization of flags marking whether a 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.

> ***Warning:***
> Use an original email address (not an alias). Otherwise emails will not be delivered in the user's inbox.

To configure the integration, follow these instructions:

1. Go to Kerio Operator Administration to section *Configuration → Voicemail → Email tab* 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.

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 drops the administrator's name and password.

Note: To synchronize flags between the two servers, Kerio Operator uses protocol IMAP with TLS or IMAPS. If Kerio Connect is behind firewall, enable at least one service on standard port. The IMAP or IMAPS services need to be allowed on Kerio Connect server.

20.4 User PIN and Email Configuration

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. On the *General* tab, enter the user's email.

> ***Warning:***
> If you integrate Kerio Operator with *Kerio Connect*, use an original email address (not an alias). Otherwise emails will not be delivered in the user's inbox.

6. Go to the *Extensions* tab and set the PIN number.

Chapter 21

Setting Emergency Numbers

Kerio Operator allows you to create a list of emergency numbers. Such numbers can be dialed even if the users are not allowed to call to 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 a predefined list of country numbers can be used.

To configure emergency calls, go to section *Configuration → Emergency Numbers* (see figure 21.1).

21.1 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 21.1).

21.2 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 21.1). Once you confirm, the numbers will be listed in the emergency numbers list. All previously configured number are rewritten but you can add more numbers manually (see section 21.1).

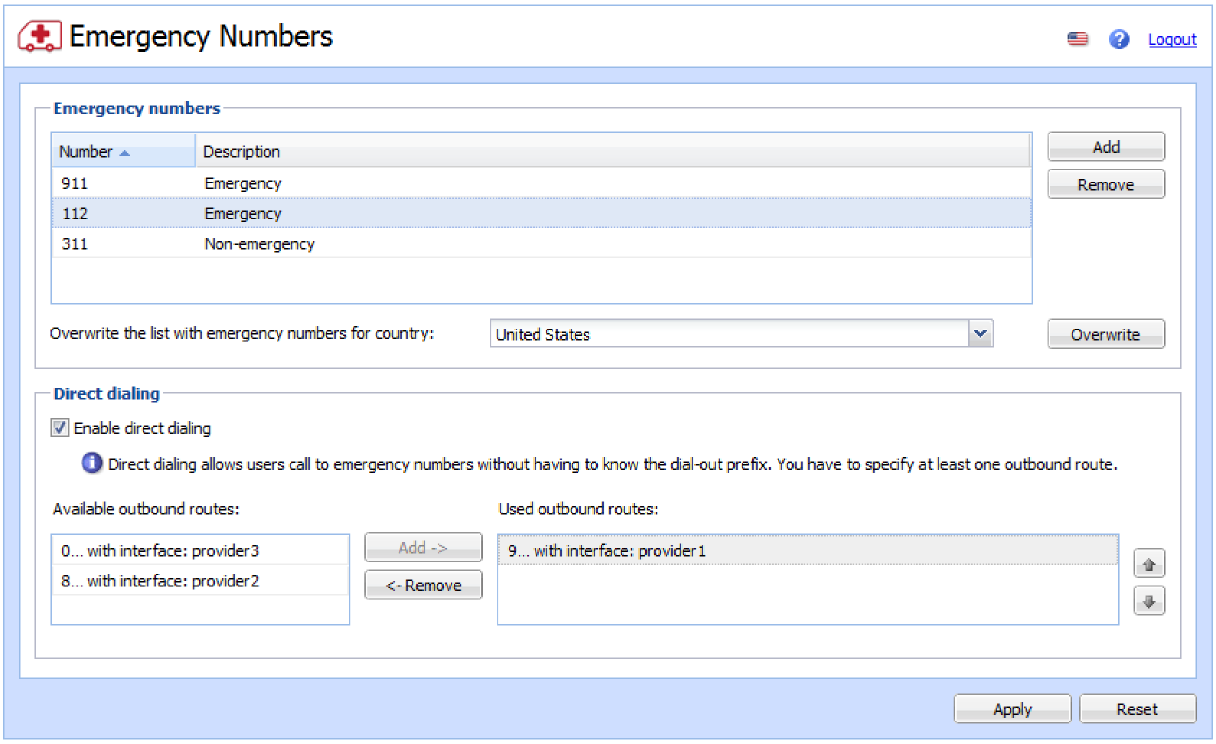

Figure 21.1 Emergency Numbers

21.3 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 one of the available outbound routes and use the *Add* button to move it (see figure 21.1).

Warning:
Emergency numbers must not 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 22

SSL Certificates

Kerio Operator allows communication encryption using SSL. The SSL encryption protocol first uses asymmetrical encryption for exchange of symmetrical 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 asymmetric 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.

22.1 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 the 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.

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

22.2 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 the 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. Select the certificate and click on the *Export* button. Save the certificate to your disk and email it to a certification organization (for example, *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode* and so on).
4. Once you obtain your certificate signed by a certification authority, go to SSL certificate section and click on Import. Import the file.
5. To enable the server to use this certificate, select the certificate and click on the *Set as Active* button.

Chapter 23
Backup

Kerio Operator supports backup of the following items:

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

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

23.1 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 recommend 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.

23.2 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 incompatibility.

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. Dialog *Recovery* opens where you select which parts of the system you wish to recover.

Chapter 24

Product Upgrade

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

1. In Kerio Operator Administration, go to section *Configuration* → *Advanced Options* to tab *Update Checker*.
2. Click on *Upload Binary Image*.

Chapter 25

Network Settings

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

25.1 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 communication.

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 must contain also the DNS server name.

If you want to change your DNS server or the method for assigning 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 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 *Packet Sniffer*.
3. This opens a dialog where you can specify what to capture. You can capture communication of 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 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).

25.2 NAT

If you use NAT in your network or at least one phone is behind NAT, read the following two scenarios:

25.2.1 Kerio Operator is in the Internet and phones are behind NAT

The scenario in figure 25.1 requires only one minor configuration in the PBX settings:

1. In the administration interface, open the *Configuration* → *Extensions* section.
2. Select the extension of the user whose phone is in a private network.
3. In the *Edit extension* dialog, go to tab *Advanced*.
4. Check the *Extension is behind NAT* option.

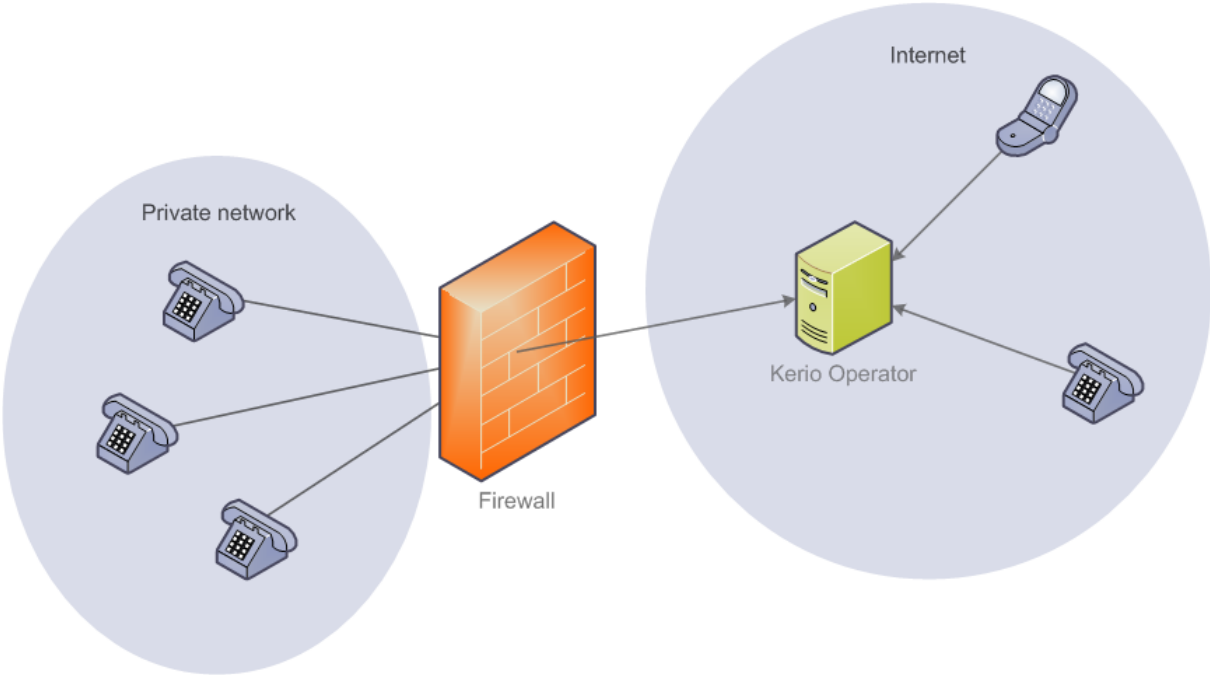

Figure 25.1 Kerio Operator is in the Internet and phones are behind NAT

25.2.2 Kerio Operator is behind NAT and phones are in the Internet

The scenario on figure 25.2 requires configuration in Kerio Operator Administration:

1. In the administration interface, open section *Configuration* → *System* → *tab Network*.
2. In the NAT support section, enable NAT by checking the option.
3. Enter the public address which should be used in SIP protocol messages.
4. For phones in the same private network as Kerio Operator, create an appropriate IP address group in section *Configuration* → *Definitions* → *IP Address Groups* with all addresses on which phones communicate in your private network. Thus, the PBX will communicate with phones within the network directly.
5. (Optional) You can also limit the RTP port range. Bear in mind that each call requires 4 ports for communication.
6. Also, map port 5060/UDP (SIP protocol) from firewall to Kerio Operator. It is usually necessary to map a port range for RTP (according to the specified interval).

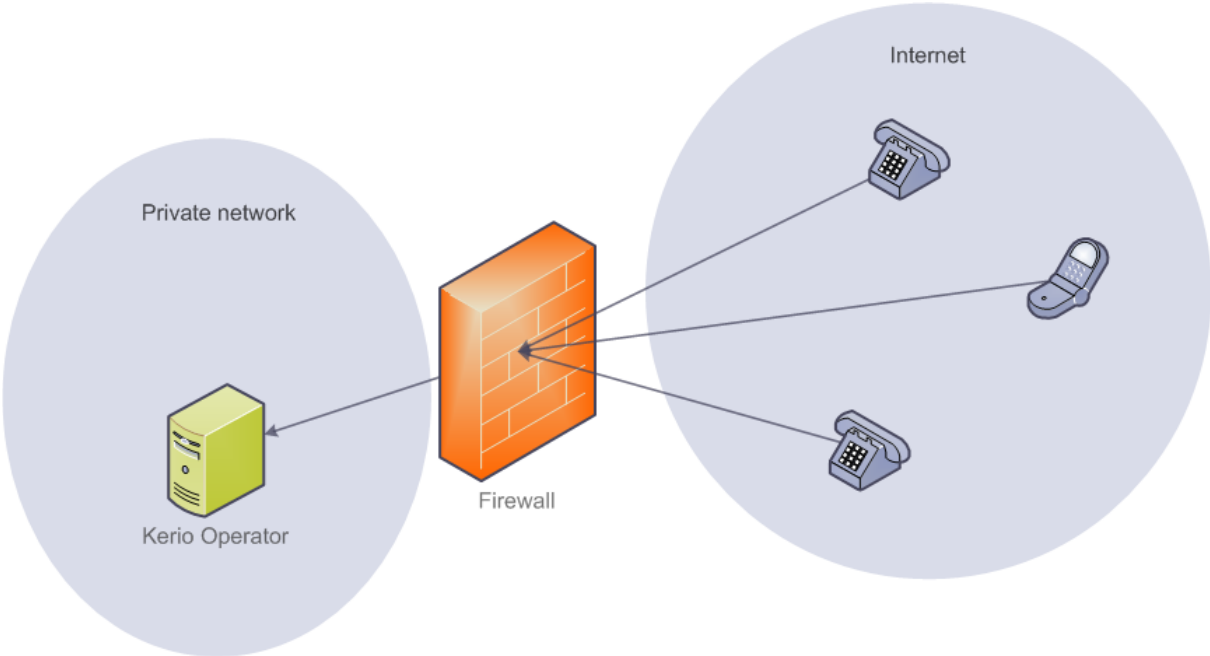

Figure 25.2 Kerio Operator is behind NAT and hardware phones are in the Internet

25.3 Firewall

Kerio Operator allows you to limit or prohibit PBX services for certain networks. To configure firewall, 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 30.

Web server

If you want to restrict connections to Kerio Operator Administration and Kerio MyPhone, check this option and select an IP group with 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 restrict the SIP protocol solely to your internal network and external IP addresses of your SIP provider.

Phone provisioning

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

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

25.4 Time Settings

Correct time and time zone settings of your PBX are necessary for correct configuration of telephone communication, time ranges and logs. If the time zone is not set properly, log messages or call history may contain confusing information. 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.

Warning:
Time and time zone settings on this tab refer to the administration interface time. It is the server time. Kerio MyPhone will display the time zone using the computer settings. If users are in a different zone to Kerio Operator, logs in call history will be displayed in users' time zone.

Chapter 26

Call Pickup

Kerio Operator supports so-called call pickup. You can configure the PBX so that a call for one extension can be answered by another extension. You can pick up call:

- among users within one group (usually people in one office),
- across groups using a special code and extension number.

Each method suits a different situation. Call pickup feature is described in detail in the following sections.

26.1 Call Pickup Rooms

In some departments in your company (for example sales department or technical support department), people sitting in one office may find call pickup very useful. Call pickup means dialing a special code on my phone (extension) to answer a call ringing on my colleague's phone (extension).

Apply settings as described below:

1. Go to section *Configuration* → *PBX Services* and enable *Call pickup*. Keep the pickup code (*8), if you do not have a reason to change it.
2. Go to section *Configuration* → *Definitions* → *Call Pickup Rooms* and use button *Add* to open dialog *Add Call Pickup Room*.
3. Enter the name of the department or the office in the *Name* field.
4. In the table, add all users and extensions that will be able to pick up calls for one another.
5. Make sure the *Room is enabled* option is checked.

26.2 Directed Call Pickup

Directed call pickup — this service enables the receptionist or personal assistants to answer calls ringing at other extensions. Imagine the following situation:

- the managing director uses extension 101
- the financial director uses 102
- they share a personal assistant

If the assistant's phone shows information that somebody is calling the managing director during his meeting with the financial director, she can accept the call by dialing `**101` and arrange a meeting for the director and the callee. Next call is for the financial director and the assistant can also accept this call. This time she dials `**102`.

As you can see, by dialing the call pickup code, you can answer a call for any extension of the PBX.

Apply settings as described below:

1. Go to *Configuration* → *PBX Services*.
2. Enable the *Directed call pickup* service.
3. Directed call pickup is now fully functional.

Chapter 27

User Rights

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

27.1 How to use prefixes to disable outgoing calls of individual users

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 one or more users. The number of such groups is not limited.

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

Groups whose calls are blocked are defined in section *Definitions* → *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 ??).

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, beer in mind that external numbers in these definitions must include the prefix for outbound calls (see chapter 6.1).

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

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 (usually with prefix 900), follow these instructions:

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 27.1.

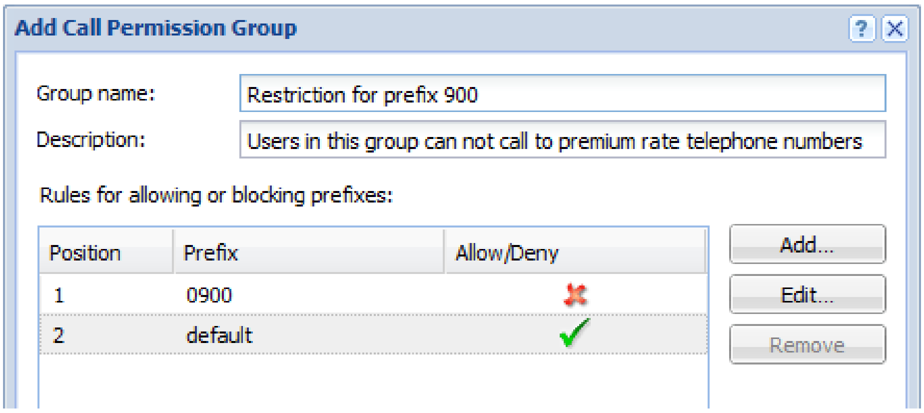

Figure 27.1 Call permission groups settings

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 restricting calls to prefix 900 by clicking *Up* (for the rule priority).

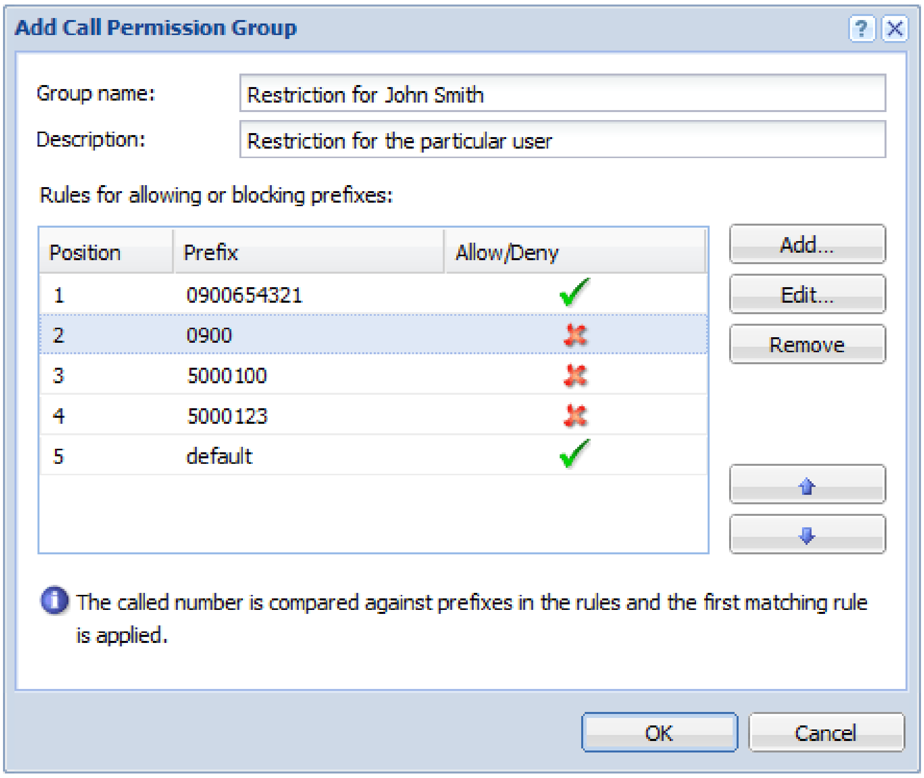

Figure 27.2 Call permission group settings for a specific user

27.2 Roles for System Access

Kerio Operator distinguishes between the following roles:

- *No rights* — user has rights to access the Kerio MyPhone interface.
- *Whole server read only* — user has rights to access Kerio MyPhone 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 32).

Chapter 28

Configuring Music on Hold

While a caller is waiting for connection or in a call queue (see chapter 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*.

28.1 Adding New Collection

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

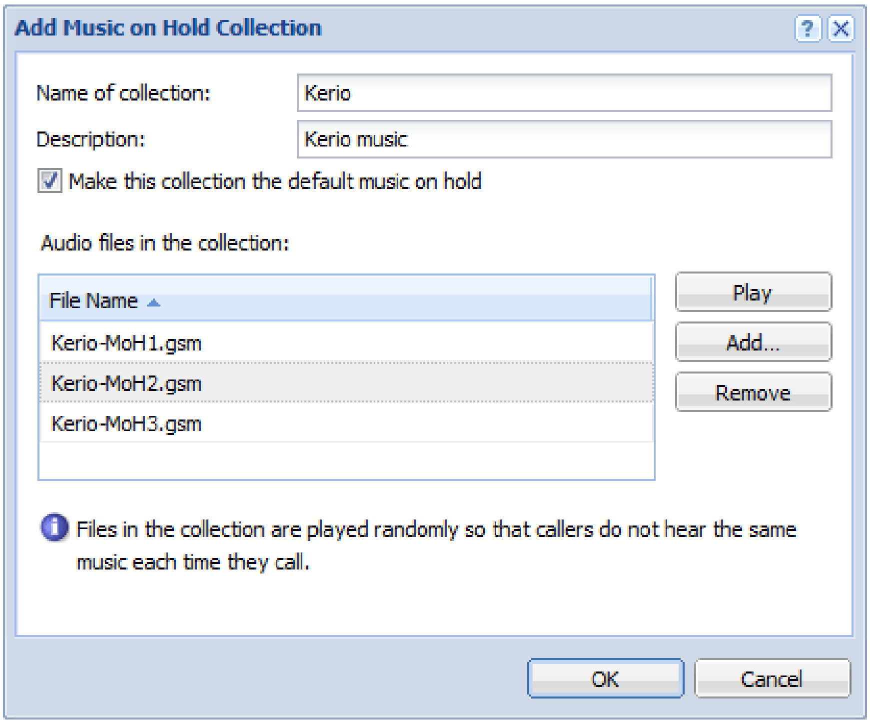

Figure 28.1 Adding New Collection

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. Repeat this step until all your uploaded files are listed in table *Audio files in the collection* (see figure 28.1).

28.2 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 29

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 17). 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 opens 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 30

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. You want to create a group of administrators who can access the administration interface only from the local network:

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 30.1).

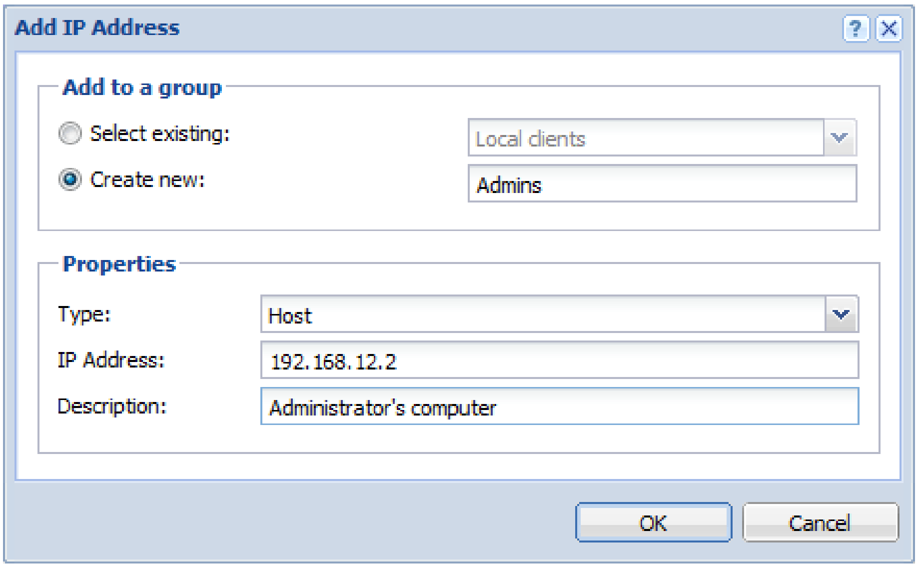

Figure 30.1 IP Address Groups Creation

6. To add more PBX administrators, click on the *Add* button on the *IP Address Groups* tab. Select the existing group *Admins* (see figure 30.2).

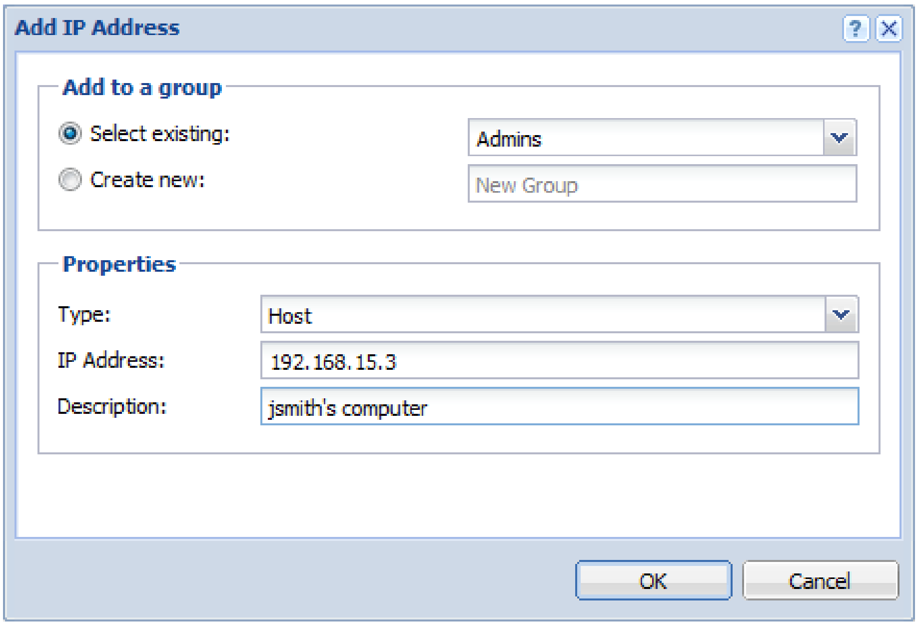

Figure 30.2 IP Address Groups Creation

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 31

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*:

31.1 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.

31.2 Viewing Active Conferences

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

31.3 Viewing Call Queues

All current calls can be viewed under *Status* → *Call Queues*. See chapter 14.2 for detailed information on viewing active call queues.

31.4 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 removed from the PBX and logs.

31.5 Monitoring Recorded Calls

Recorded calls can be monitored or played under *Status* → *Recorded Calls*. For information on recording and playing calls, go to chapter 14.2.

31.6 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 a 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.

You can also create new tasks there. Just click on the *Add*:

Restart All Phones
With this option, you can plan a specific time for automatic restart of provisioned phones.

Periodically Remove Old Recorded Calls
With this option, recorded calls can be periodically removed so that there is always enough space on the disk (calls from queues can be recorded).

31.7 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* to reboot or power off any planned tasks (see section 31.6) 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 opens a dialog with information about disk usage of audio files, voicemail and configuration file of Kerio Operator.

Chapter 32

Logs

Logs are files where information about certain events (e.g. error and warning reports, debugging information, etc.) is 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.

32.1 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).

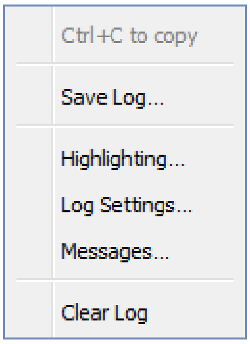

Figure 32.1 Context menu

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.

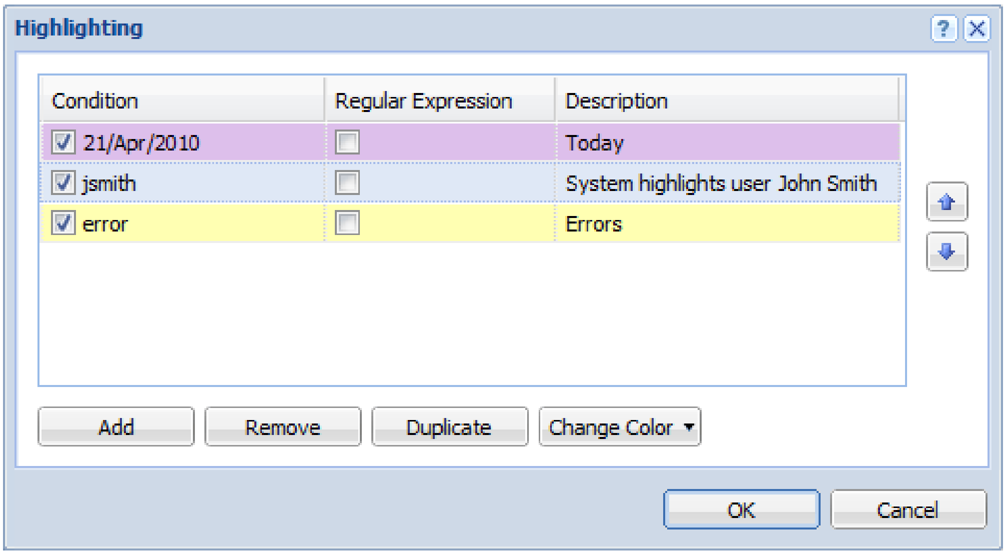

Figure 32.2 Highlighting

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

- *Condition* — every line containing the substring specified will be highlighted according to the parameters set in this dialog.
- *Regular expression* — enter any regular expressions in the *Condition* field[3] (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.

[3] 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 Operator* 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.

32.2 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 user logins/logouts to/from Kerio Operator administration

Example:

```
[11/Jan/2012 08:35:53] Admin - session opened for host 127.0.0.1 from
Web Administration.  User-Agent:  Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:8.0) Gecko/20100101 Firefox/8.0.
```

- `[11/Sep/2012 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 from Web Administration` — information about session opening and IP address of the user logged in and that they are logged in to administration.
- `User-Agent:  Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0.` — information about the browser and operating system versions of the computer from which the user is connected to Kerio Operator.

Changes in the configuration database

Changes performed in the administration interface. Let's take a user removal as an example:

```
[11/Jan/2012 08:35:53] Admin - Removed User {"GUID":4,"USERNAME":"jwayne"}
```

- `[11/Sep/2012 08:35:53]` — the date and time of the log creation
- `Admin - Removed User {"GUID":4,"USERNAME":"jnovak"}` — action that was executed: user `Admin` removed user with username `jwayne`.

32.3 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 pieces of information. Select those you need. Selection can be done as follows:

1. Right-click on the log screen and select option *Messages* 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.

32.4 Error

In contrast to the *Warning* log, the *Error* log displays errors of great significance that usually affect the application's operation. Kerio Operator administrator should check this log regularly and fix detected problems as soon as possible. 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.

32.5 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.

32.6 Security

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

32.7 Warning

The *Warning* log displays warning messages about errors of little significance.

Events recalling warning messages in this log do not seriously affect the PBX functionality. However, they can point at current or possible problems. The *Warning* log can help if for example a user is complaining that certain services are not working.

Chapter 33

Notifications

Kerio Operator uses notifications in the right top corner to inform you about important system actions (see figure 33.1). The following events are displayed:

- New version of Kerio Operator is available.
- The dial plan has been changed. It is necessary to restart provisioned phones to update the configuration file.
- Core dump has been generated — a critical error has occurred and it is necessary to send the file to the technical support of *Kerio Technologies*.

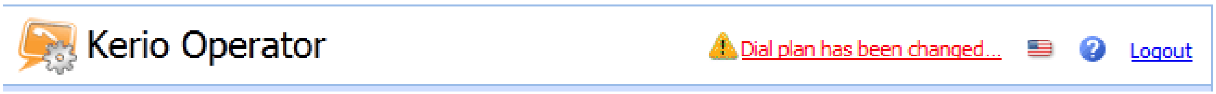

Figure 33.1 The area for displaying notification

You can click the notification and learn how to solve the problem.

A notification disappears once the problem is solved.

Chapter 34

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://forums.kerio.com/ and the knowledge base that can be found on http://kb.kerio.com/.
- Specific issues can be asked via a special technical support form at http://support.kerio.com/.

34.1 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 00 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.

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.

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.

Kerio Asterisk Module

The Kerio Asterisk Module extends the functionality of the Asterisk PBX to match *Kerio Operator* needs. It is distributed and licensed under GNU General Public License version 2. Complete source code is available at:

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

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.

libiconv

Libiconv converts from one character encoding to another through Unicode conversion.

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.

The library is available for download at:

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

libxml2

XML parser and toolkit.

OpenLDAP

Freely distributable *LDAP* (*Lightweight Directory Access Protocol*) implementation.

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.

PHP

PHP is a widely-used scripting language that is especially suited for Web development and can be embedded into HTML.

This product includes PHP software, freely available from http://www.php.net/software/

ScoopyNG

This product includes software developed by Tobias Klein.

tftpd

TFTP daemon. TFTP is a simple protocol used for file transmission.

zlib

General-purpose library for data compressing and decompressing.