Porta Switch™

New Features Guide

Maintenance Release 19

Copyright Notice & Disclaimers

Copyright © 2000-2009 PortaOne, Inc. All rights reserved

PortaSwitch: New Features Guide, April 2009
Maintenance Release 19
V1.19.9

Please address your comments and suggestions to: Sales Department, PortaOne, Inc. Suite #408, 2963 Glen Drive, Coquitlam BC V3B 2P7 Canada.

Changes may be made periodically to the information in this publication. Such changes will be incorporated in new editions of the guide. The software described in this document is furnished under a license agreement, and may be used or copied only in accordance with the terms thereof. It is against the law to copy the software on any other medium, except as specifically provided in the license agreement. The licensee may make one copy of the software for backup purposes. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopied, recorded or otherwise, without the prior written permission of PortaOne Inc.

The software license and limited warranty for the accompanying products are set forth in the information packet supplied with the product, and are incorporated herein by this reference. If you cannot locate the software license, contact your PortaOne representative for a copy.

All product names mentioned in this manual are for identification purposes only, and are either trademarks or registered trademarks of their respective owners.

Table of Contents

Preface

This document describes new features found in PortaSwitch Maintenance Release 19.

Where to Get the Latest Version of This Guide

The hard copy of this guide is updated at major releases only and does not always contain the latest material on enhancements introduced between major releases. The online copy of this guide is always up-to-date and integrates the latest changes to the product. You can access the latest copy of this guide at: **www.portaone.com/support/documentation/.**

Conventions

This publication uses the following conventions:
- Commands and keywords are given in **boldface**
- Terminal sessions, console screens, or system file names are displayed in `fixed width font`.

Caution indicates that the described action might result in program malfunction or data loss.

NOTE: Notes contain helpful suggestions about or references to materials not contained in this manual.

Timesaver means that you can save time by performing the action described in the paragraph.

Tips provide information that might help you solve a problem.

1. New Features in PortaBilling100

Overdraft Protection

The traditional authorization scheme, in which the system checks the amount of available funds at the beginning of a call, has many drawbacks. For one, the system does not react to balance changes (refunds, payments, or charges) made while the call is in progress. Since every session is authorized based on the total amount of resources available, overdrafts are possible in the case of multiple concurrent sessions and the like.

This is why PortaBilling now offers you the ability to dynamically lock the funds required to pay for a certain amount of a service before that service is used. Proper implementation of overdraft protection requires support both on the billing engine side (PortaBilling) and on the part of the network element providing the service, e.g. PortaSIP. (See below for a description of the scenarios applicable to "legacy" switches.)

Authorization and fund locking

What is the relationship between authorization and fund locking? Authorization is simply a check as to whether the currently available funds are enough to cover a service (or how much of the service can be used with the funds currently available). Using a simple analogy, it is like taking a look in your wallet to see how much money you have left before deciding whether you have enough money to purchase a DVD or buy some chocolate bars. The problem is that such a check is done without taking into account your other attempted purchases. For example, if you have $20 available, the system will tell you that you have enough money to buy 1 DVD ($15) or 10 chocolate bars ($2 each); but it cannot tell you whether you can buy a DVD and also buy 3 chocolate bars.

Fund locking not only checks that you have enough money for the DVD, but also immediately puts that money into a different compartment of your wallet. Now when you check to see how many chocolate bars you can buy, you will only be working with the remaining portion of the money. This will spare you an awkward situation at the cash register.

Dynamic authorization

The simplest overdraft protection scenario is "resource locking". This is done when an application knows the amount of funds required beforehand. So right at the start the application sends a request to validate the availability of these funds and, if this is successful, it locks them. Then, when the purchase has been completed, a "charge" event is sent to PortaBilling. One example of such a service is pay-per-view content distribution. After a customer clicks on a "Get the movie" link, the system authorizes and locks the funds to cover the cost of the movie, in order to

ensure that the customer has the right permissions and sufficient funds. The customer is then shown a confirmation screen. If he approves the purchase, the money is deducted from his account

Dynamic re-authorization is a more complex process, which is used when it is not possible to tell how much a customer will spend in a particular session, so that additional funds have to be locked "on the go". When a session (e.g. a voice call) starts or is in progress, the system "reserves" a small portion of the available funds to cover the next time interval (e.g. 5 minutes). As the end of this interval comes near, the system attempts to reserve funds to cover the next interval, and so on. If no remaining funds are available, the call is disconnected. So if a customer sends an SMS message during a phone call (decreasing the available funds), or makes a credit card payment (increasing the available funds), this will immediately affect the call – either it will be disconnected sooner, or the maximum allowed call time will increase.

Let's see how dynamic re-authorization works in a specific example, where an account is concurrently using multiple services and making a payment while the session is still in progress.
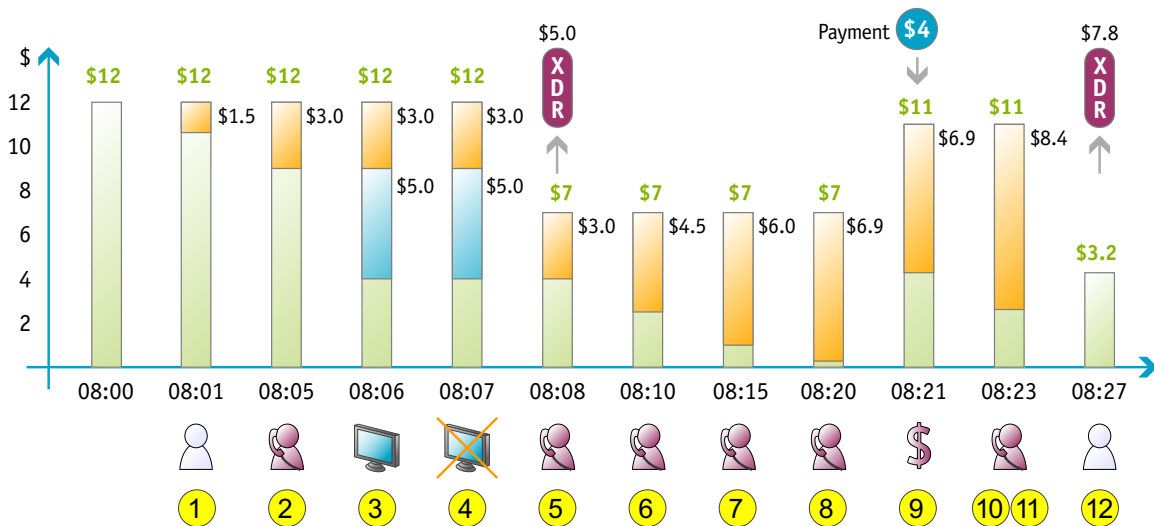
- Initially, the account has $12 available.
- The user starts a phone call to a destination with a price of $0.30 per minute. The PortaSIP server requests call authorization for 5 minutes. At this point the user's balance is still unchanged, but funds covering a 5-minute phone call ($1.50) are locked (**1**).
- While the call is in progress, at some time before the end of the "approved" period (for our example, we'll assume this is one minute), the PortaSIP server will attempt to perform re-authorization.

- PortaSIP sends a re-authorization request to billing. PortaBilling verifies that the account has enough funds for another 5 minutes. The amount locked is now $3.00 (**2**).
- While still on the phone, the user decides to purchase a pay-per-view movie. An authorization request arrives from the IPTV platform, and the funds needed to pay for the movie ($5.00) are locked in addition to the previous $3.00 (**3**).
- The user now attempts to purchase another movie ($5.00), but this request is rejected, since he only has $4.00 left (**4**).
- The purchase of the first movie is completed, and the balance decreases to $7.00 (**5**).
- Since the call is still in progress, and the end of the "authorized" time is approaching, PortaSIP sends another authorization request, and so funds for another 5 minutes are locked (a total of $4.50 is now locked) (**6**).
- The user keeps talking, and so 5 minutes later yet another authorization is sent. The total amount of locked funds is now $6.00 (**7**).
- Soon another authorization is sent, but now there are only enough funds for 3 minutes. $6.90 is now locked (**8**).
- The user realizes that he is running out of money, but wants to continue the phone call, and so he promptly makes an online payment with his credit card. $4.00 is deposited to his account (**9**).
- Since the last re-authorization provided less time than requested (3 minutes instead of 5), PortaSIP determines that the user is out of money, and normally it would disconnect the call. However, it makes one last re-authorization attempt, one minute before the call is to be disconnected (**10**).
- Since the user now has available funds, another 5 minutes of call time are authorized. The total amount of locked funds is now $8.40 (**11**).
- Finally, the user disconnects, and is charged $7.80 for the full call duration of 26 minutes. Thus his balance is now $3.20 (**12**).
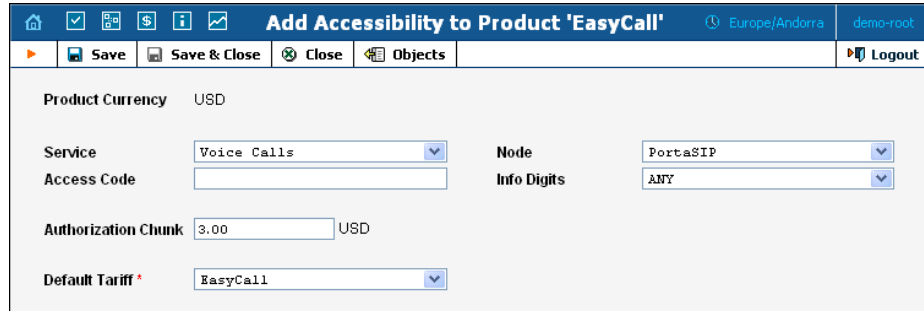
Authorization chunk

Two situations may lead to an excessive locking of funds:

- Attempting to use an "expensive" service – For instance, let's assume that PortaSIP is configured to lock sufficient funds for a 15-minute conversation at the start of a call. This is fine for calls to US or Europe (in which case just 20-40 cents would be locked). But if a customer with a fairly low balance calls an expensive destination (e.g. Somalia – $1.00/min), he may find that all of his funds are suddenly locked up, and will not be able to use another service in the meantime.
- Old-style applications that do no support re-authorization – If an authorization request comes from a gateway or switch which does

not support dynamic fund locking, then all the available funds will be locked while that session is in progress.

To prevent locking too many or all available funds, the administrator can configure the product's **Authorization Chunk** parameter.
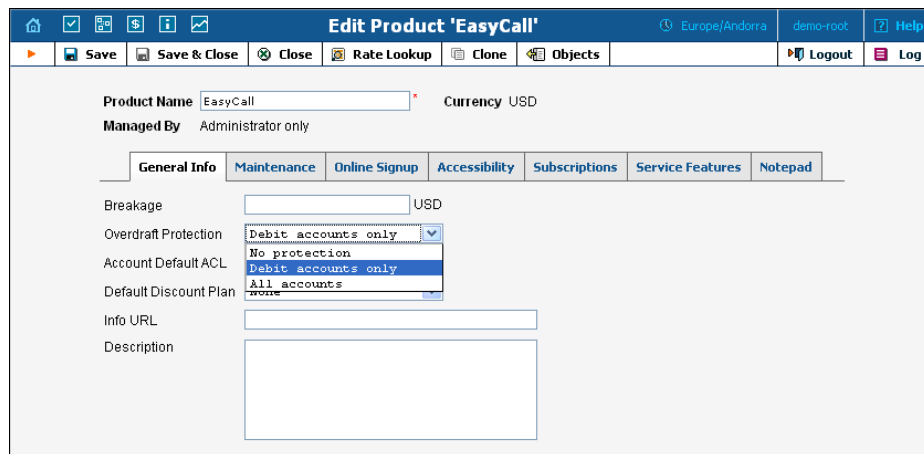

Then each request will lock up no more than the amount specified there. Taking our example of a call to Somalia, if we set the authorization chunk to $3.00, the billing engine will respond to PortaSIP's request to lock funds sufficient for 15 minutes by locking up only $3.00 (3 minutes). Thus PortaSIP will perform authorization every three minutes.

Legacy equipment and backward compatibility

What happens when a node that is not capable of dynamic re-authorization sends a "standard" RADIUS authorization request? Also, how does fund locking affect the previously available "fraud protection" feature in PortaBilling (where a debit account is allowed to make only one simultaneous call)?

Answer: the product configuration features an **Overdraft Protection** setting, which allows you to fine-tune how fund locking is applied:

- **None** means that there are effectively no "locked" funds. When a locking of funds is requested, these locks will be done separately

for each session, and will not affect other sessions. So there can be several concurrent sessions, and each can potentially use up all the available funds. This method thus provides transparency for the application using overdraft protection, although in reality it does not provide greater security than a simple authorization request. It is analogous to "Fraud Protection Off" mode in previous releases. For obvious reasons, it is not recommended for general use.

- **Debit accounts only** – In this case, no fund locking will be done for credit accounts, while for debit accounts the requested amount will be locked. When an authorization request is received from a "legacy" application for a debit account, the billing engine will lock either all of the available funds on that account, or only the Authorization Chunk amount. This is identical to PortaBilling's default behavior in Maintenance Release 18 and older.

- **All accounts** – This is used where fund locking is done for all account types. For "overdraft protection-aware" applications, the amount of funds locked is the smaller of either the amount needed to cover the requested service amount, or the **Authorization Chunk**. For legacy authorization requests, it is either all of the available funds, or the **Authorization Chunk**. This is probably the most secure mode, but it may be too restrictive in the case of legacy equipment.

NOTE: Currently, overdraft protection only operates with funds available on the account level, i.e. you can use it for debit accounts and credit accounts that have an explicitly defined credit limit.

Routing Plan Selection

When a customer makes an outgoing phone call, he is charged according to a tariff chosen based on the accessibility entry. Various accessibility points can be defined, and different tariffs can be applied to each of them. This means you can charge a customer differently based on where a call originates (e.g. a call to the US originating from an IP phone connected to PortaSIP is charged $0.04/min, while a call to the same phone number in the US would be charged $0.06/min if made by dialing a toll-free access number from the customer's landline phone).

At the same time, you may have different termination vendors with various prices and levels of audio quality. What, then, if you want to give your customers the freedom to choose, i.e. whether to make phone calls via low-cost carriers (and thus pay low rates), or use high-quality carriers (and so pay premium rates)? This is now possible in Maintenance Release 19. Each type of routing (low-cost, premium, etc.) is defined as a separate routing plan, and multiple routing plans can now be associated with a single accessibility entry in the product definition. A specific tariff can be

assigned to each routing plan, and this tariff will be used when a customer subscribing to a specific plan places a call.
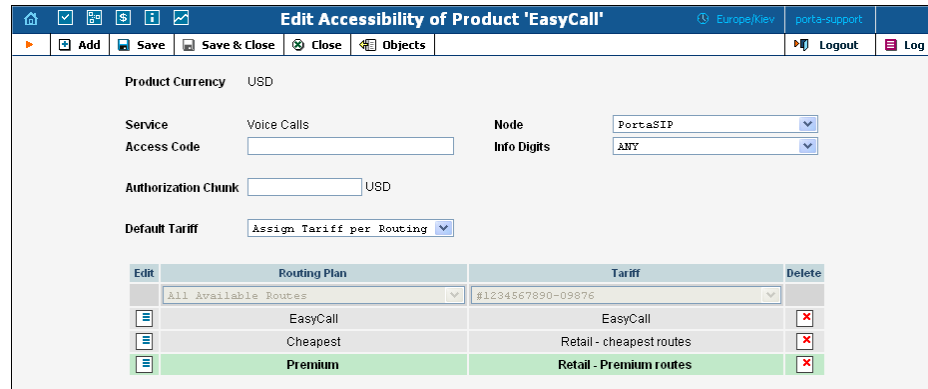

Selecting a specific routing plan

There are two possibilities for choosing which routing plan is used to find available vendors and terminate a call:

- Each account is assigned a default routing plan. When the end-user simply dials a number in the normal way, this routing plan will be used. In PortaSwitch Maintenance Release 18 and older, "Routing Plan" was the property of a customer. Now it has been removed from the customer, and is available to each account individually.
- If the end-user wants to choose a specific routing plan for a particular call, he dials a routing plan selection code before the number. For example, if he wants to use the "Premium" routing plan to call US phone number 12065551234, he would dial 02312065551234, where 023 is the selection code defined as a property of the "Premium" routing plan.

Selection codes

The selection code is a property of a routing plan, and so obviously each routing plan has its own unique selection code. If you want to have a routing plan which cannot be specifically selected by an end-user, simply leave the selection code field empty.
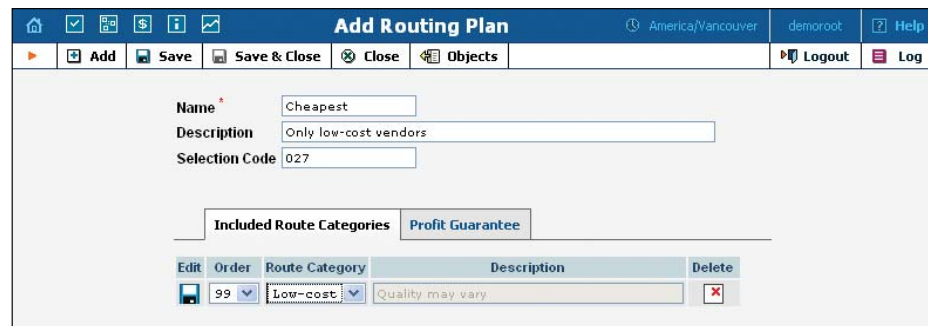
The old mode (single tariff per accessibility entry) has been kept for backward compatibility and faster performance when real-time selection of routing plans is not required. In this case, you can still assign a default routing plan to an account, and this will be used when the end-user makes a phone call. However, it is not possible then to use selection codes. The "single tariff" mode is active by default when you create a new accessibility entry. If you wish to apply a specific tariff based on which routing plan is used, you need to manually switch on the "Tariff Selection" option in the accessibility settings.

Dialing Rules

By including a routing plan in the accessibility definition, you potentially allow every account with this product assigned to it to use this routing plan. If you want to prohibit a specific customer from selecting this routing plan for a call, you can disable it in the customer's dialing rules. In that case, calls will be routed using the account's default routing plan.
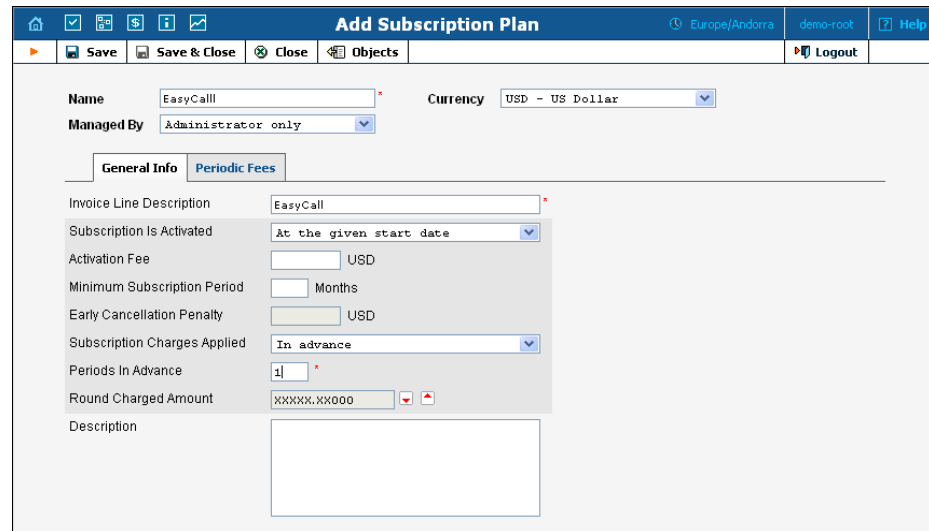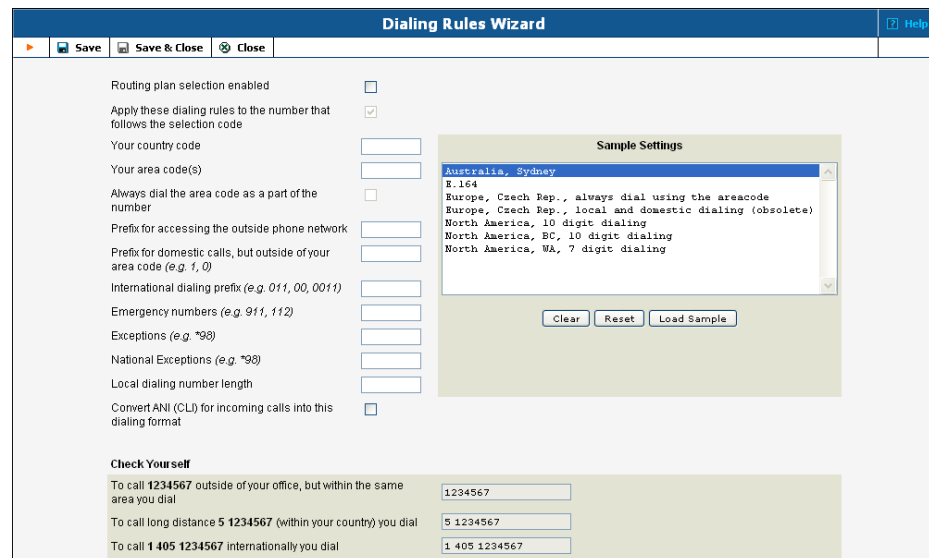

Subscriptions Charged in Advance

While a customer would normally be invoiced for his service-related activities (e.g. phone calls or messaging) after the service has been rendered, many service providers would like to charge the subscription fees in advance, in order to improve their cash-flow and minimize the potential loss when a customer leaves without paying his last bill.

Other subscription types ensure that when a customer's billing period is closed, he is charged until the end of that billing period. The new "In advance" mode of charging subscription fees ensures that, at the end of

the billing period, the customer is charged until the end of the Nth full billing period following the current one. So if we charge one month in advance and the current monthly billing period ends on April 10th, the customer will be charged until May 10th, and his invoice produced on April 11th. will contain charges for calls made prior to April 10th and subscription charges covering the period from April 11th. to May 10th.

Pro-rating for advance charges

If a subscription which is charged in advance is not active during the whole billing period, it is pro-rated in the same way as post-charged subscriptions are. For instance, if a customer with a monthly billing period activates a "1 month in advance" subscription in the middle of his billing period (e.g. on March 17th.), the invoice issued to him on April 1st. will include subscription fees from March 17th. to April 30th. (i.e. the incomplete portion of the current billing period and the whole next billing period).

If a customer terminates a subscription prior to the end date of a period that has already been charged (e.g. the customer in the example above closes his account on April 20th), then a refund will be issued for the "unused" subscription time when the billing period is closed.

Internet Access Service

PortaBilling now fully supports the provisioning of an Internet access service (DSL, ADSL, PPPoE) for Cisco BRAS and other compatible equipment. A PortaBilling administrator can provision the amount of available bandwidth per product or individual account and also perform static IP allocation for certain accounts. All these settings are then returned to the access server during authentication, and so will be applied

to the session. The Internet access service can be charged based on either total connection time or the amount of data transferred.

2. New Features in PortaSIP

Rate Limit for Incoming SIP Messages

To protect an ITSP from a denial-of-service attack or service degradation when a SIP device erroneously starts sending PortaSIP a stream of false SIP messages, PortaSIP can now dynamically track the rate at which it is receiving data from each IP address. If - by mistake, or with malicious intent - a certain device starts sending too many packets at once, these packets will be blocked so that other users can continue using the service normally.

Busy Lamp Field (BLF)

This highly popular IP Centrex feature extends PortaSIP's presence capability to popular modes of "business" IP phones (e.g. Polycom), so that a secretary can see the line status of other extensions. So far this feature has been tested on the Linksys 962+932, Snom 320 and Polycom IP 550 phones.

3. New Features in PortaUM

Voice-to-text Service

PortaUM is now integrated with the GotVoice service to provide "visual voicemails" to customers. When someone leaves a voicemail for a user who is subscribed to the IP Centrex and unified messaging services on PortaSwitch, this message is stored (as a sound file) in the user's PortaUM mailbox. The user cannot retrieve this message via his phone or web browser; rather, to get the information contained in the message, he needs to listen to it.

Voice-to-text is an add-on to the unified messaging service. Once a recorded voice message is delivered to PortaUM, it can be transferred to one of the GotVoice servers for processing. GotVoice uses state-of-the-art technology to recognize message contents, combining computerized speech recognition with live human assistance for those parts which cannot be processed automatically. In a matter of minutes the customer receives an email containing a transcript of the message text. This makes it possible to access the voicemail information via an email client or an SMS sent to a mobile phone.
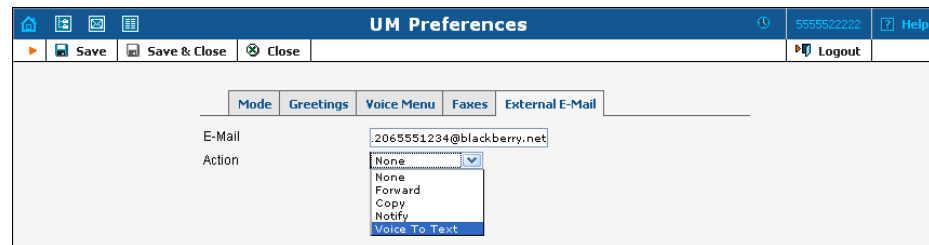

VoIP providers using PortaSwitch can now reliably offer subscribers the ability to read their voicemail and process the information instantly. Using this service requires a contract with GotVoice (in order to be assigned an account giving access to the conversion API) and the basic PortaSwitch configuration (to create rates for this service, etc.).

Since this is a paid service, PortaUM performs authorization in PortaBilling prior to conversion (to verify that the customer has sufficient funds). Once conversion has been completed, it sends a "charge" event to PortaBilling.

Fax-only UM Account

Normally, a party calling a voice mailbox or auto-attendant menu in PortaUM can start a fax transmission at any time. PortaUM automatically detects this and switches to "receive fax" mode.
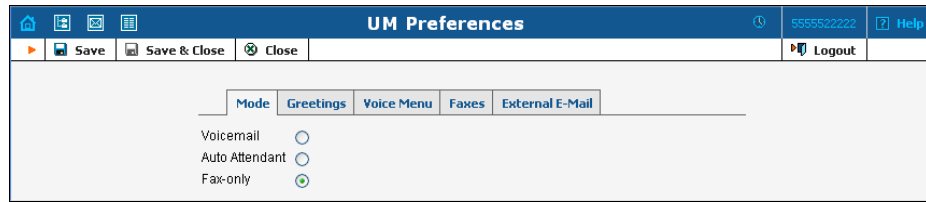
In some cases, this could confuse users unfamiliar with modern communications, who may expect to hear a fax tone before pressing the start button on their fax machine. "Fax-only" is a special setting for the PortaUM mailbox which helps avoid such situations. When an incoming call is connected, it immediately provides the "fax negotiation" tones, thus prompting the other side (human or fax machine) to initiate transmission. This enables easy migration of legacy fax services to the PortaSwitch IP Centrex platform.