

PortaSwitch

New Features Guide

62

MAINTENANCE
RELEASE



Copyright Notice & Disclaimers

Copyright © 2000–2017 PortaOne, Inc. All rights reserved

PortaSwitch® New Features Guide, April 2017
Maintenance Release 62
V1.62.09

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. The 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 for 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	4
Custom Ringback Tone	5
Incoming SMS Message Delivery	6
Percentage-Based Forwarding of Incoming Calls	7
Transfer of Funds and Airtime Among End Users	9
Support of P-Access-Network-Info Header	11
IPv6 Network Configuration in PortaSwitch®	15
Token-Based API Authentication for Resellers and Retail Customers....	16
Other Features and Enhancements	16
Web Interface Changes	22
Important Upgrade Notes	23

Preface

PortaSwitch® Maintenance Release 62 is the next leap-forward release, consistent with our “fast releases, precisely on time” ideology.

Where to get the latest version of this guide

The hard copy of this guide is updated upon 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`.



Exclamation mark draws your attention to important actions that must be taken for proper configuration.

NOTE: Notes contain additional information to supplement or accentuate important points in the text.



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



Archivist explains how the feature worked in previous releases.



Gear points out that this feature must be enabled on the Configuration server.

Tips provide information that might help you solve a problem.

Trademarks and Copyrights

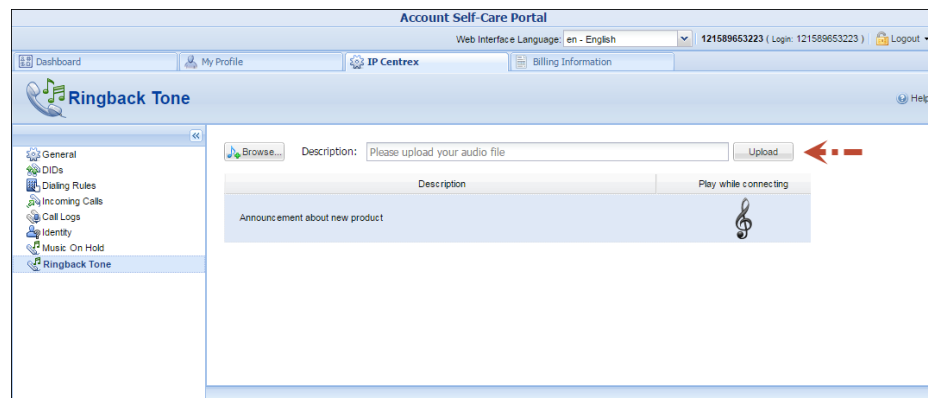
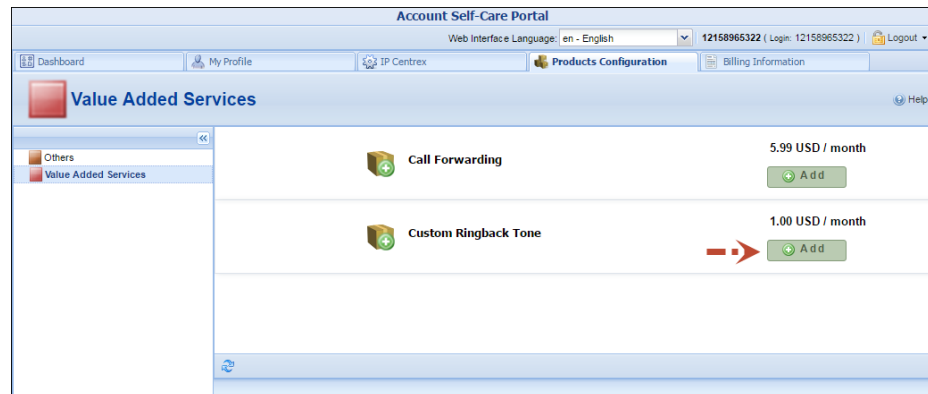
PortaBilling®, PortaSIP® and PortaSwitch® are registered trademarks of PortaOne, Inc.

Custom Ringback Tone

Custom ringback tone, a very popular service offering, allows end users to replace ordinary ringback sounds with either music or a greeting of their choice. It is extremely attractive to users nowadays to the point where many service providers regard it as a must-have service offering.

Beginning with this release, the custom ringback tones are fully supported by PortaSwitch®.

Let's say that customer John Doe runs an advertisement campaign and wants a caller to hear a customized announcement instead of the standard ringback tone. On his account self-care interface, John Doe subscribes to the Custom ringback tone add-on product and uploads the custom announcement media file to the **Ringback Tone** page. The system encodes the uploaded file with the G.711, G.729 and G.723 codecs and then saves these files to its internal storage.

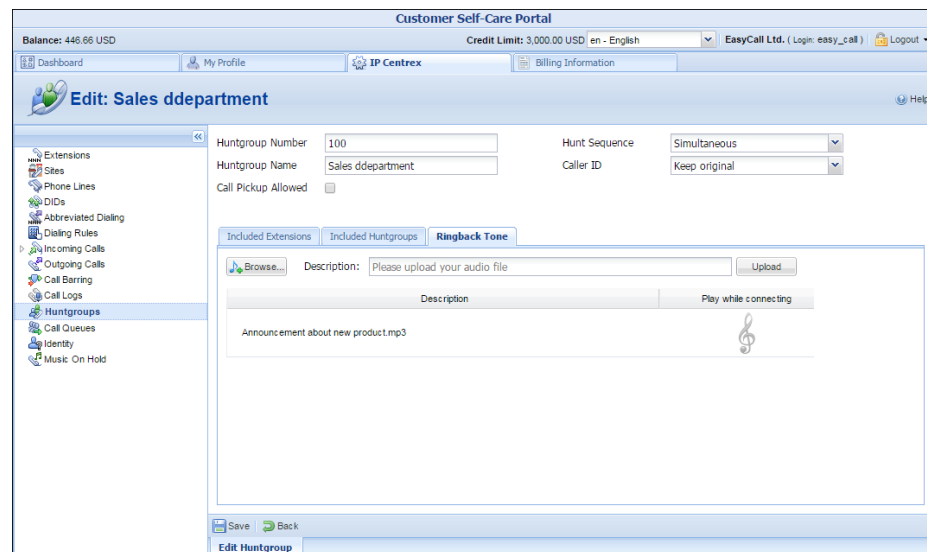


John Doe receives an incoming call and the custom announcement file is streamed to the caller.

NOTE: Encoding the uploaded files with G.711, G.729 and G.723 codecs and copying them to storage requires a certain amount of time to complete (around 5 minutes). Therefore, although the custom track is shown as having been successfully uploaded to the web interface during this period, the standard ringback tone plays for calls.

PortaSwitch® does not send custom ringback tones for calls made through IVR applications. In these cases, the caller hears media played by a corresponding IVR application.

Along with individual users, custom ringback tones can also be set up for huntgroups.



This allows service providers to offer this increasingly popular service to their customers and thereby gain an additional revenue stream.

Incoming SMS Message Delivery

More and more people use mobile applications in their daily life. To gain these users as customers, service providers can now introduce a two-way SMS service that allows them to enjoy exchanging messages with their friends and family.

With this release, PortaSwitch® accepts incoming SMS messages from mobile operators and delivers them to end users within the network.

All incoming SMS messages for recipients are free of charge, while the sender of the SMS message is the one charged per message.

Incoming SMS handling is determined by the *domain service policy* configuration. Thus, when PortaSIP® receives SMS messages via the SMPP protocol, the delivery flow looks like this:

1. PortaSIP® matches the corresponding domain service policy (using a domain pattern) that defines how the SMS message must be processed.
2. PortaSIP® authorizes the message in PortaBilling® and receives instructions to deliver the message to the end user within the network.
3. PortaSIP® converts the SMPP message to the SIP protocol and routes it to the account within the network.
4. If the recipient is online, they immediately receive the message. If not, PortaSIP® stores the message until the recipient comes online (their application registers them within the network) and then delivers the message.

Together with outgoing messaging, this full-scale solution allows service providers to benefit from this two-way SMS service, as it adds additional profit.

Percentage-Based Forwarding of Incoming Calls

Sometimes customers use the services of outsourced call centers to handle their incoming calls in different cities or states, etc. Since call centers can be of different sizes and in various geographical locations, customers need to define how many calls to forward to this or that call center due to cost requirements and / or business contracts.

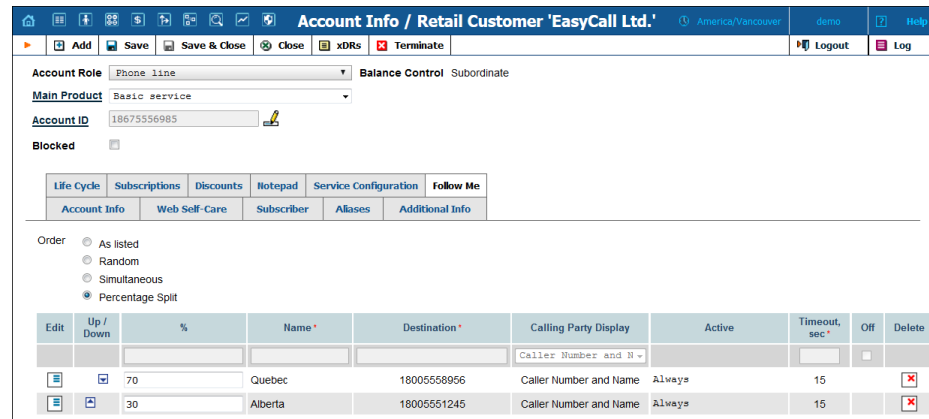
With this release, it is now possible to configure PortaBilling® to forward incoming calls to external phone numbers, percentagewise. This makes the configuration for call forwarding more flexible and allows service providers to meet customers' more specific needs.

For example: Let's say your customer is an online shop whose main phone number is 18675556985. They have signed an agreement with and use the services of a Canadian call center to handle their incoming calls. The call center has a big office in Quebec (18005558956) and a smaller one in Alberta (18005551245). Since the Quebec office has more employees, that office can potentially handle more calls and thus 70% of incoming calls to 18005556985 must be forwarded to them while 30% of incoming calls must be forwarded to their Alberta office.

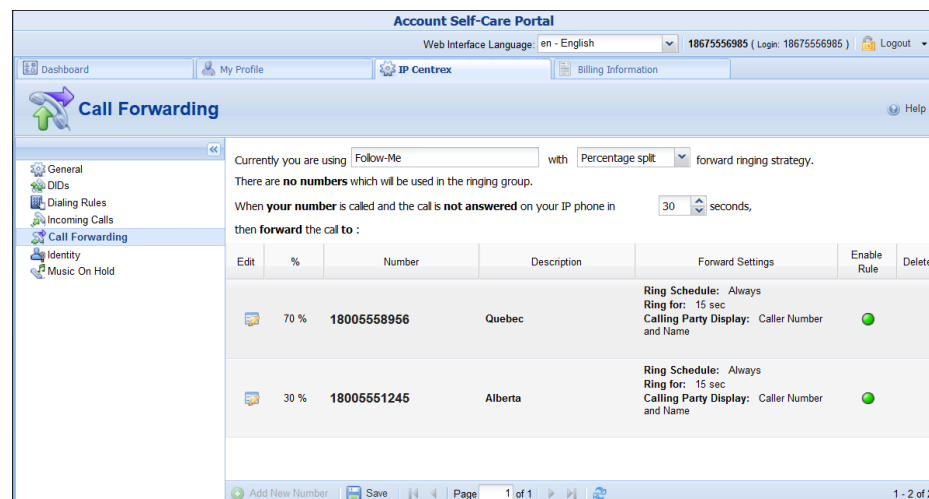
To configure PortaBilling® to forward a customer's incoming calls to several phone numbers, percentagewise, administrators must first enable the **Call Forwarding** service feature and then specify either the **Follow Me** or the **Advanced Forwarding** mode. On the **Follow Me** tab of the

Account Info page, select the **Percentage Split** order control and configure the forwarding parameters.

NOTE: The total percentage for all forwarding phone numbers equals 100%, therefore when adding forwarding numbers, the percentage for the first entry is always 100. Administrators can change the percentage when adding the next forwarding number.



If a customer prefers to perform percentage-based forwarding by themselves on their self-care interface, an administrator must first enable the **Call Forwarding** service feature. Then, on the **Call Forwarding** page the customers can select the **Percentage Split** forward ringing strategy and add the forwarding parameters.



This feature allows service providers to fine-tune their customers' incoming handled calls and reallocate the incoming calls among several call centers. This new feature expands the number of outsourcing call centers that their customers may use.

Transfer of Funds and Airtime Among End Users

Transfer of funds and airtime among end users is a very popular service, especially in countries where payment systems are scarce. Money transfers provide a fast and convenient way to pay for everything without cash and / or credit cards.

With the transfer of funds and airtime feature, end users are able to:

- transfer their available funds to pay for goods and services, and
- share airtime from their service wallets with friends and family.

End users can take advantage of this service via their self-care interface. They can select what to transfer: either money or airtime (minutes, SMSs, GB, etc.) from their service wallet. Then they enter the recipient's phone number. For security purposes, each time a user initiates a transfer, the system sends an email or an SMS with a verification code. This code expires in 3 minutes and becomes invalid after the 3rd ineffective attempt to enter it. This is a safety provision to protect users from unauthorized persons obtaining access to verification codes.

As soon as an end user inputs a verification code to the system and the operation is successful, funds or airtime are transferred to the recipient.

Account Self-Care Portal

Balance: 145.00 USD

Web Interface Language: en - English | 17781235015 (Login: 17781235015) | Logout

Dashboard | My Profile | IP Centrex | Products Configuration | Billing Information

Transfer Funds

- Billing Summary
- Products and Services
- Quotas and Service Wallets
- Volume Discounts
- Transactions
- Top-up with Voucher
- Mobile Payment Transfer
- Transfer Funds**
- Make a Payment
- Payment Info

Action

- Transfer Main Balance Funds
Available Funds: 145.00 USD
- Transfer Service Wallet contents
Service Wallet: Canada (Messaging Service) - 30 messages
 UK (Voice Call) - 200 minutes

Back | Next

Account Self-Care Portal

Balance: 150.00 USD

Web Interface Language: en - English | 17781235015 (Login: 17781235015) | Logout

Dashboard | My Profile | IP Centrex | Products Configuration | Billing Information

Transfer Funds

- Billing Summary
- Products and Services
- Quotas and Service Wallets
- Volume Discounts
- Transactions
- Top-up with Voucher
- Mobile Payment Transfer
- Transfer Funds**
- Make a Payment
- Payment Info

Transfer Service Wallet contents

Service Wallet: Canada (Messaging Service)

Available messages: 30

Recipient: David Green - 17781235025

Amount to transfer: messages

Comment:

Verification Code:

Back | Transfer

Let's consider a transfer of funds and airtime, separately.

Transfer of funds

To prevent fraud, the administrator only enables the transfer of funds for an individual customer or a customer class.

End users who have debit accounts can transfer their available funds from their self-care interfaces. This is very convenient, since it encourages them to manage their funds efficiently, and be ready to either top-up their relatives' balances or pay for goods in a shop.

For instance, let's say the user Richard Roe has \$50 worth of available funds. He decides to transfer \$35 to pay for goods in a grocery store. Richard Roe visits his self-care interface, enters the phone number of the grocery-store owner and the amount of money to be transferred – \$35 in this case. He receives an SMS with a verification code and immediately enters that into the system. The system accepts the code and funds are withdrawn from his account. The grocery-store owner receives \$35 and Richard's available funds are now \$15.

Transfer of airtime

Transfer of airtime involves the transfer of the contents of any service wallet – minutes for calls, SMSs, GB of Internet traffic, etc. The transfer is only allowed among end users having identical volume discount plans. This is a safety measure to prevent service abuse (e.g. when end users sign up for cheap products and then transfer airtime to use for premium products or commercial purposes).

Service providers encourage end users to make frequent top-ups to provide for the transfer of airtime.

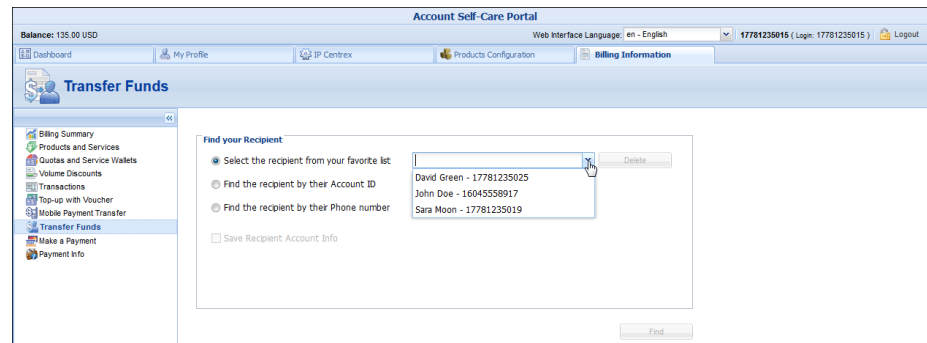
For instance, Jane Smith and her friend have identical service wallets that include Voice calls and Internet traffic. As the friend spent all his service wallet balance on Internet traffic, Jane Smith transfers 2 GB so they can continue chatting via the Internet. Afterwards, Jane finds out that her own service wallet ran out of money too, so she tops up her service wallet.

Favorites list

End users may create a favorites list that includes recipients they are accustomed to cooperating with. The list is easy to manage, and transferring funds and / or airtime can be done with just a few clicks. This saves time and makes the transfer process more user-friendly.

For example, returning to Richard Roe, let's say he visits the grocery store every week and pays for his goods by transferring funds. To have the grocery-store owner's contact information at hand, he includes it in his

favorites list. Next time he goes grocery shopping he just selects the owner's account from the list and transfers the money. It's that simple and efficient.



Implementation specifics

In conclusion, the transfer of funds and airtime feature has the following implementation specifics:

1. Both sender and recipient must be allowed to transfer funds.
2. Only debit accounts can transfer and receive funds.
3. The currency of the sender and recipient must be the same.
4. To allow debit accounts to transfer and receive funds, enable this option either at the customer or customer class level.
5. Only accounts with identical service wallets can transfer and receive airtime.
6. To allow airtime exchanges, enable this option within the service wallet.

With this solution, service providers can increase their revenue by encouraging their end users to frequently top up their service wallets and their main balance to be ready for transferring money to their families and friends. Since no payment system is required to transfer funds and / or airtime, the service is widely used.

In addition to being an easy and secure way to pay for goods and services it encourages users to register new accounts. Thus, service providers also expand their customer base.

Support of P-Access-Network-Info Header

According to some European countries' regulations (e.g. France's legal requirements), service providers must send caller location information to their termination partners. This information contains the operator's code who processes the call and the code of the city where the call originates (the INSEE code in France).

To meet these requirements, PortaSwitch® now supports the PANI (P-Access-Network-Info) SIP header. This header contains caller location information and is added to outgoing INVITE requests. Thus, PortaSwitch® either generates the PANI value for an account or relays the value received during an incoming call.

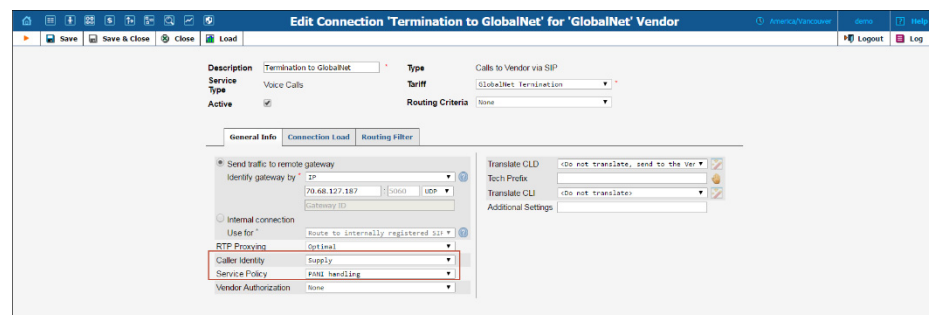
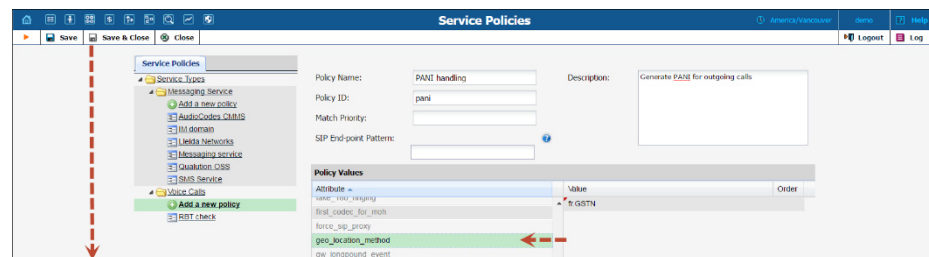
Note that caller location information is sensitive. Therefore, your vendors who send / receive the PANI header must adhere to privacy regulations and be capable of correctly processing privacy information.

Support for PANI is determined by the service policy attribute **geo_location_method**. When combined with further system configurations, it determines how to process a call.

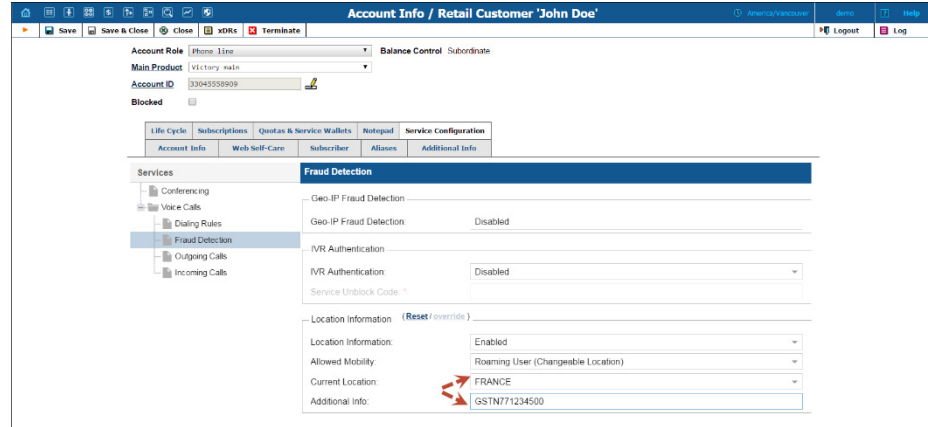
Let's have a closer look at how it works:

PANI generation by PortaSwitch®

To supply the PANI to a vendor when an account makes a call, the administrator configures the service policy and assigns it to this vendor's outgoing connection. The connection that correctly processes privacy information is therefore marked as "trusted" (its **Caller Identity** option is set to **Supply**).



The administrator also defines the location within the account's configuration by using the **GSTNR1R2C1C2C3C4C5XX** pattern, where: **GSTN** is the network definition, **R1R2** is the service provider's individual code, **C1C2C3C4C5** is the city code, and **XX** are auxiliary digits (00 by default).



So then, when John Doe makes an outgoing call, the INVITE request to the vendor will contain the extra PANI header:

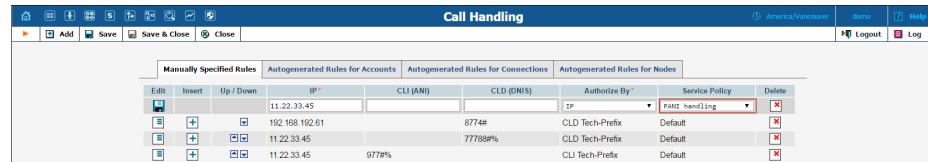
```
From: "John Doe" <sip:33045558909@sip.example.com>;
tag=53qq3i7fo6eymuap.o
P-Access-Network-Info: GSTN;operator-specific-
GI="771234500";network-provided
```

where GSTN and 771234500 values are taken from John's location information.

PANI relay by PortaSwitch®

In wholesale service provisioning, calls that arrive to your network already contain PANI that is supplied by your customers. In these cases, PortaSwitch® must obtain the PANI and relay it to the vendor.

To do this, the administrator configures a service policy and assigns it to a corresponding call handling rule.



Then the customer's location is defined and the account is configured to trust the caller's identity (the **CLI Trust** option is set to **Caller only**).

Account Role: [IPv4 address]

Main Product: [happy_traffic]

Account ID: [11.22.33.45]

Blocked:

Account Info | Add-on Products | Web Self-Care | Subscriber | Additional Info | Life Cycle | Service Configuration

Services

- Voice Calls
 - Dialing Rules
 - Fraud Detection
 - Outgoing Calls
 - Incoming Calls

Service Policy: []

Fair Usage Policy: []

Fair Usage Policy: Disabled

Music on Hold: (Reset/override)

Music on Hold: Enabled

File: No Frits Cumbia (c) 2001 Kevin MacLeod, Latin

CU Trust: (Reset/override)

Accept Caller Identity: **Caller Only**

Supply Caller Identity: Yes

Limit Simultaneous Calls: []

When the customer's account makes a call, PortaSIP® extracts the PANI and adds it to the outgoing INVITE request:

```
From: Amanda Smith
<sip:33089123000@11.22.33.45>;tag=y6reils4nf5oqkol.o
P-Access-Network-Info: GSTN;operator-specific-
GI="887854200";network-provided
```

If, for some reason, the customer is unable to provide the PANI, the administrator defines the default value for the customer:

Account Role: [IPv4 address]

Main Product: [happy_traffic]

Account ID: [11.22.33.45]

Blocked:

Account Info | Add-on Products | Web Self-Care | Subscriber | Additional Info | Life Cycle | Service Configuration

Services

- Voice Calls
 - Dialing Rules
 - Fraud Detection
 - Outgoing Calls
 - Incoming Calls

Fraud Detection

Geo-IP Fraud Detection: []

Geo-IP Fraud Detection: Disabled

IVR Authentication: []

IVR Authentication: Disabled

Service Unblock Code: []

Location information: (Reset/override)

Location information: Enabled

Allowed Mobility: Stationary User (Permanent Location)

Current Location: **FRANCE**

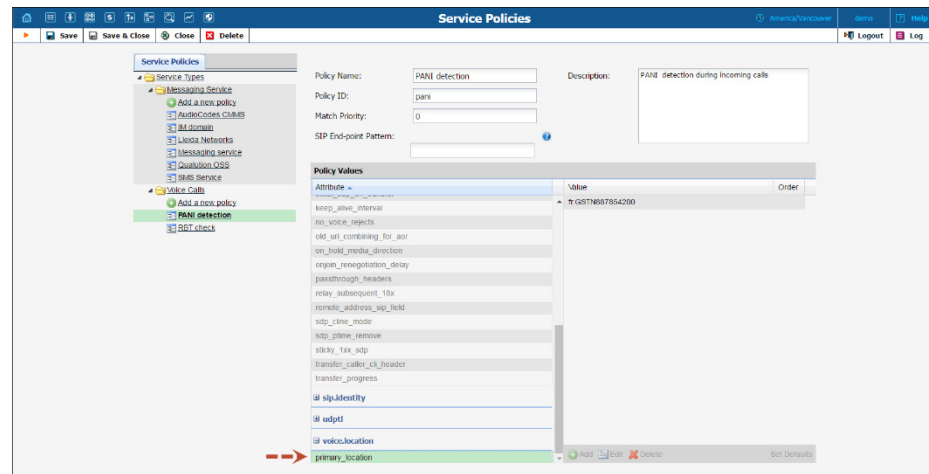
Additional Info: **GSTN887854200**

In this case, PortaSwitch® generates the PANI and sends it to the vendor, as described above.

PANI handling for incoming calls

When an incoming call arrives from an external network, it already contains the PANI provided by the vendor. Therefore, PortaSwitch® must be configured to detect and process the PANI, or, if the PANI is absent or invalid, override it with a valid one.

This is done by adding a **primary_location** value to the service policy for the incoming vendor connection.



As with outgoing requests, the connection to deliver incoming calls must properly process privacy information (set the **Caller Identity** option to **Accept**).

When someone calls John Doe, PortaSwitch® receives the following INVITE:

```
From: Jane Smith <sip:33129990215@sip.mycompany.com>;
tag=qlxm7q4vltbfg6ew.o
P-Access-Network-Info: GSTN;operator-specific-
GI="886854200";network-provided
```

If John Doe does not answer the incoming call and has forwarding correctly configured, PortaSwitch® will forward the call with the PANI to John's mobile phone.

This enhancement ensures legitimate service provisioning for service providers in the European Union.

IPv6 Network Configuration in PortaSwitch®

The evolution of the Internet and the growing number of IP devices now demands making the transition to IPv6.

With this release, PortaSwitch® supports two network interfaces – IPv4 and IPv6. This enables administrators to both add and modify IPv6 addresses on servers, and obtain network configuration information about either interface.

Both of the network interfaces operate in parallel, although the IPv4 network interface remains the primary one.

This enhancement is a preliminary step for the “dual-stack” mode in PortaSwitch® and provides possibilities for the gradual migration of servers from an IPv4 network to an IPv6 network.

Token-Based API Authentication for Resellers and Retail Customers

You can now use API tokens to authenticate reseller and customer applications (e.g. CRM systems) that are integrated with PortaBilling® via API.

To enable token-based authentication, select the **API token access** checkbox on the **Web Self-Care** tab for a particular retail customer or reseller.


The screenshot shows the 'Edit Customer' interface for 'John Doe'. The 'Web Self-Care' tab is selected. The 'API token access' checkbox is checked, and the 'API authentication token' is displayed as '45b9d857-bf37-46ec-b71f-b'. A red box highlights the 'Allow login from' section, which is set to 'Specific IP addresses/networks' with the list: 192.168.192.128/30; 61.232.6.164; 81.27.212.130.


Then adjust the application to use the combination of the API token and login.

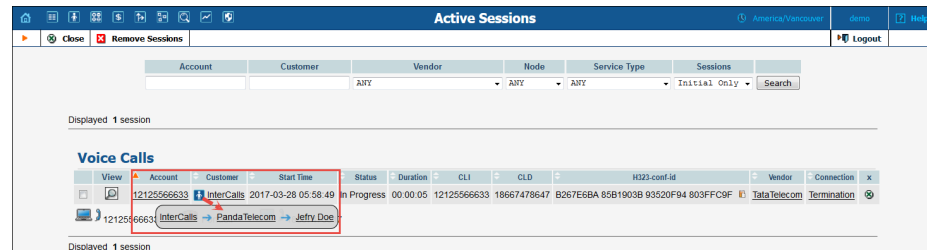
In addition, you can restrict access to PortaBilling® from specific IP addresses / networks. This increases the security in application communications with PortaBilling® plus eliminates the chance for malicious activities to take place in your system.

Other Features and Enhancements

- **Improved presentation of active sessions** – With this release, administrators can see a full chain of the resellers, subresellers and their customers that are involved in a single call.

To differentiate among the active calls of your direct customers and those of your resellers, the  **Participants** icon has been added on the **Active Sessions** page. It indicates calls that are made by your resellers' customers.

If a subreseller's customer makes a call, the name of the top-level reseller is placed in the active calls table. Also, you can see the full chain of entities involved in a call by clicking the  **Participants** icon.

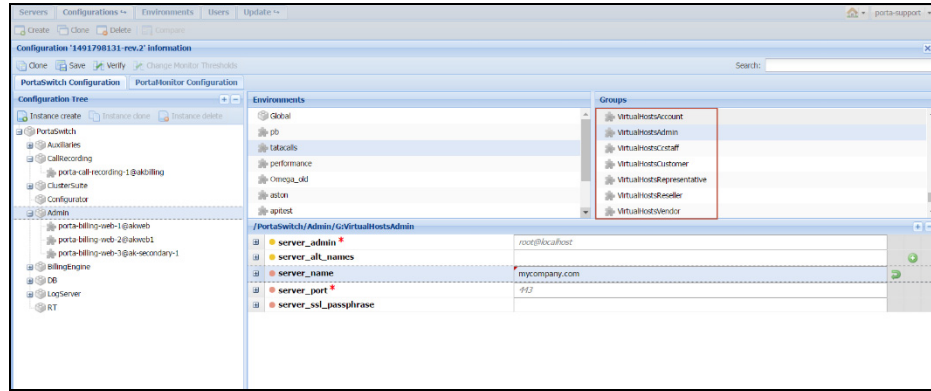


The screenshot displays the 'Active Sessions' page. At the top, there are navigation icons and a 'Logout' button. Below the navigation bar, there are filters for Account, Customer, Vendor, Node, Service Type, and Sessions. A search bar is also present. The main content area shows a table of active sessions. Below this, there is a 'Voice Calls' section with a table of call records. A red box highlights a call record with the following details: Account: 12125566633, Customer: InterCalls, Start Time: 2017-03-28 05:58:49, Status: In Progress, Duration: 00:00:05, CLI: 12125566633, CLD: 19667478647, H323-conf-id: B267E6BA 85B1903B 93520F94 803FFC9F, Vendor: TataTelecom, and Connection: Termination. A red arrow points to the 'InterCalls' customer name, and a red box highlights the 'Participants' icon next to it.

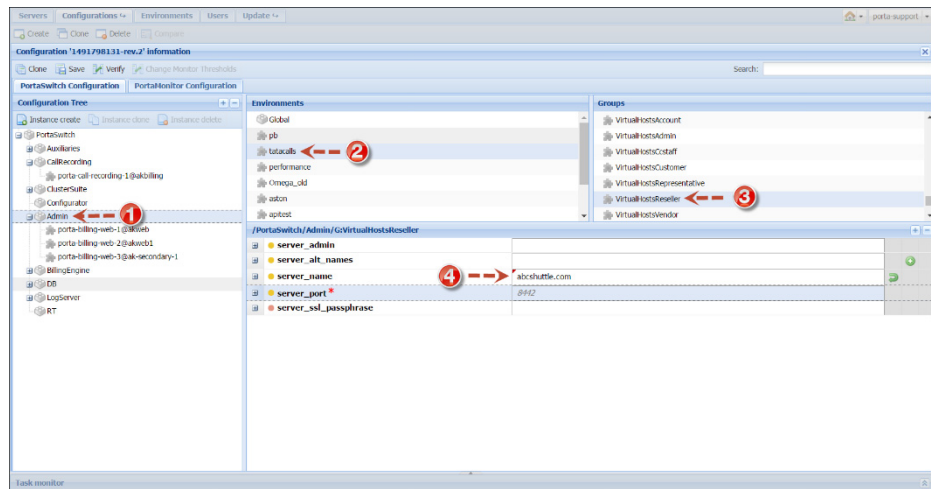
This enhancement allows administrators to differentiate among calls made by their direct customers and those made by the customers of their resellers / subreseller's. Thus the traffic flow is clearer and more evident and the monitoring process is also simpler.

- **Enhanced configuration of virtual hosts** – Quite often, service providers who provide hosting services must brand billing environments for their customers' usage. They may wish to customize access for different types of users (e.g. resellers), in addition, by using a dedicated domain name.

These goals are reached by adding virtual hosts to the web server for each billing environment and / or realm, i.e. type of user. If this is done manually, it imposes an additional load on administrators and could potentially lead to a misconfiguration due to human error. Therefore, virtual hosts are now added to individual realms per billing environment via the Configuration server web interface.



So, to brand PortaBilling® for the hosting customer TataCalls, the administrator selects the `tatacalls` billing environment and configures `tatacalls.com` as the server name for admin access. Similarly, if reseller ABC Shuttle requires customized access to PortaBilling®, the administrator selects the **VirtualHostsReseller** group and configures `abcshuttle.com` as the server name within.

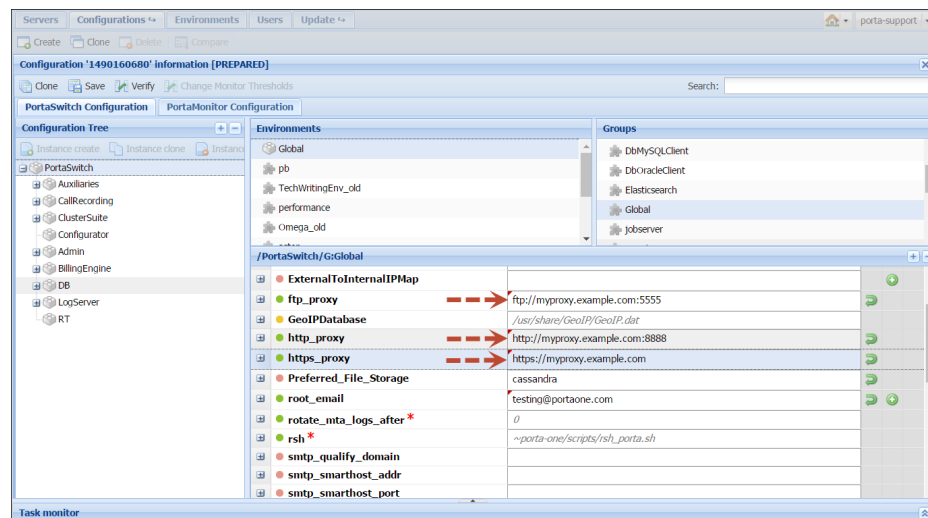


In this way, service providers perform effective system management while reducing the load on administrators.

- **Porter enhancements** – This release introduces the following enhancements in billing data transfer by using Porter:
 - Extended xDR history transfer – Now you can transfer xDRs that contain additional information about particular calls (e.g. information about the extension to which the call was redirected or the real caller identity, etc.), xDRs produced for on-net calls, and those created for unsuccessful attempts. This provides a clearer idea of a customer’s activities upon import.
 - CPE and SIM inventory records transfer – This enhances account data transfer and saves you from having to

- preconfigure CPE devices and SIM cards within the target system. Note that you must still pre-configure CPE profiles.
- A custom fields transfer is accomplished either as part of the customer class configuration or separately. This adds flexibility to customer management.
 - **Web proxy definition via the Configuration server** – Typically, a web proxy serves as a mediation component in the communications between local and remote hosts. This provides a better security model and protects your network, since hosts can send requests via the web proxy and remain anonymous to each other.

With this release, you can instruct PortaSwitch® to send outgoing HTTP(s) and / or FTP requests (e.g. to query a payment processor's API) through a web proxy server on the Configuration server web interface. The defined proxy is global and applies to all servers within the system.



The system preserves your settings with each network configuration update, thus reduces the load on your administrators.

This enhancement gives you additional flexibility in network management and further increases the security for your network.

- **Improved re-rating procedure for imported CDRs** – Administrators can import CDRs to PortaBilling® from various external sources by using the xDR Mediation utility.

The utility extracts the CDRs from incoming files and arranges the ready for processing CDRs into collections. PortaBilling® calculates the charges for these CDRs according to defined rates, and then based on this information, creates transaction records (also called xDRs). The created xDRs are then associated with corresponding accounts and vendors.

If an issue occurs during charge calculation (e.g. due to incorrect rate definition), the utility marks those CDRs as being rejected. This alerts an administrator to an issue that occurred at the rating stage.

The screenshot shows the 'CDR Mediation' utility interface. At the top, there are navigation icons and a title bar. Below the title bar, there are filters for Status (ANY), Date (For 24 hours), and a date range (From: 2017-03-11 00:00:00, Till: 2017-04-11 13:47:53). There is also a checkbox for 'With rejected CDRs only'. Below the filters is a table with the following columns: xDRs, CDR Collection, Status, Added, Processed, Total Records, Imported, Skipped?, and Rejected?. The table contains five rows of data, with the last row having a red arrow pointing to the 'Rejected?' column.

xDRs	CDR Collection	Status	Added	Processed	Total Records	Imported	Skipped ?	Rejected ?
	20170411_1045_2333600001134_0001	Processed	2017-04-11 13:45:45	2017-04-11 13:45:54	1	1	0	0
	20170411_1052_1302100001385_0001	Processed	2017-04-11 13:52:53	2017-04-11 14:07:25	1	1	0	0
	20170411_1114_2780800001850_0001	Processed	2017-04-11 14:14:58	2017-04-11 14:20:33	1	1	0	0
	20170411_1134_2780800002635_0002	Processed	2017-04-11 14:34:24	2017-04-11 14:46:30	1	0	0	1
	20170411_1148_3143900001042_0001	Processed	2017-04-11 14:48:09	2017-04-11 14:48:45	1	0	0	1

The administrator can adjust the rating configuration and re-run the rating process for the rejected CDRs.

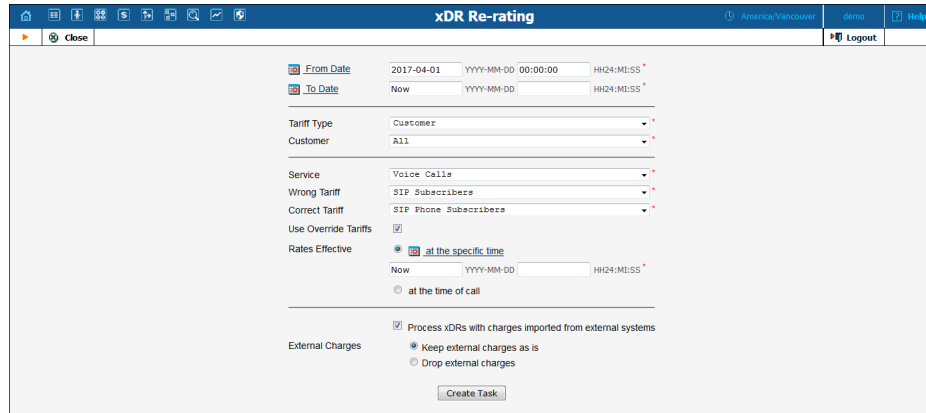
With this release, the xDR Mediation utility prevents the creation of xDRs when an issue occurs during charge calculation. The administrator detects the rejected CDRs on the **CDR Mediation** page and can re-run the rating process. Upon successful execution, the administrator will only find re-processed xDRs on the account / vendor **xDR History** pages.

This prevents xDR duplication from occurring when the re-rating procedure takes place.

- **Enhanced re-rating of xDRs with external charges** – Service providers may import xDRs that already contain charged amounts to PortaBilling®. Beginning with this release, administrators can choose how to handle those xDRs during the xDR re-rating procedure.

To re-rate xDRs that contain already charged amounts, administrators enable the **Process xDRs with charges imported from external systems** option on the **xDR Re-rating** page.

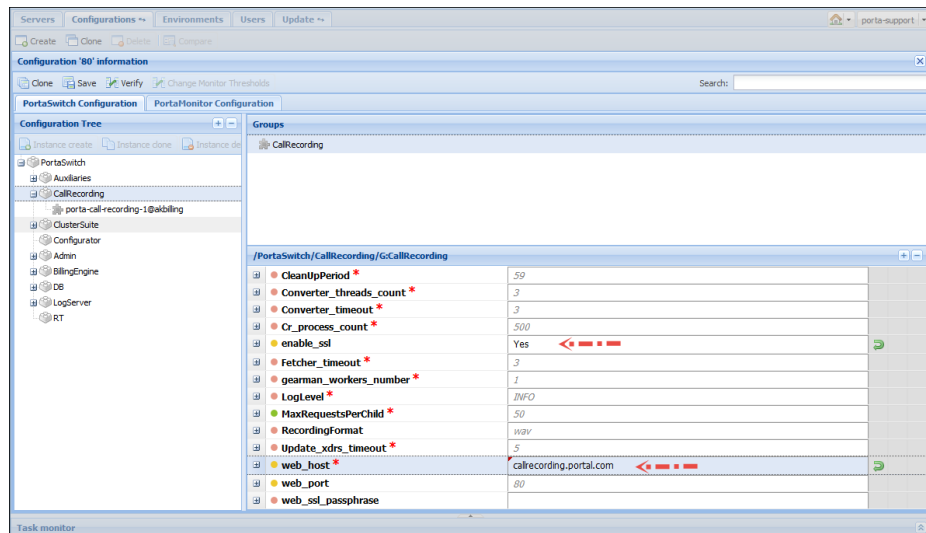
Then, to add the price from the tariff to the externally charged amount, select **Keep external charges as is**. To reset the charged amount and calculate charges using the price from the tariff, select **Drop external charges**.



This enhancement lessens the system load and speeds up the re-rating procedure.

- **Customize access to the call recording server** – Service providers use domain names to enable users to access their web sites. With this release, administrators can easily customize access to their call recording server using the domain name.

To do that they specify the subdomain resolved to their call recording instance’s IP address in the **web_host** option on the Configuration server.



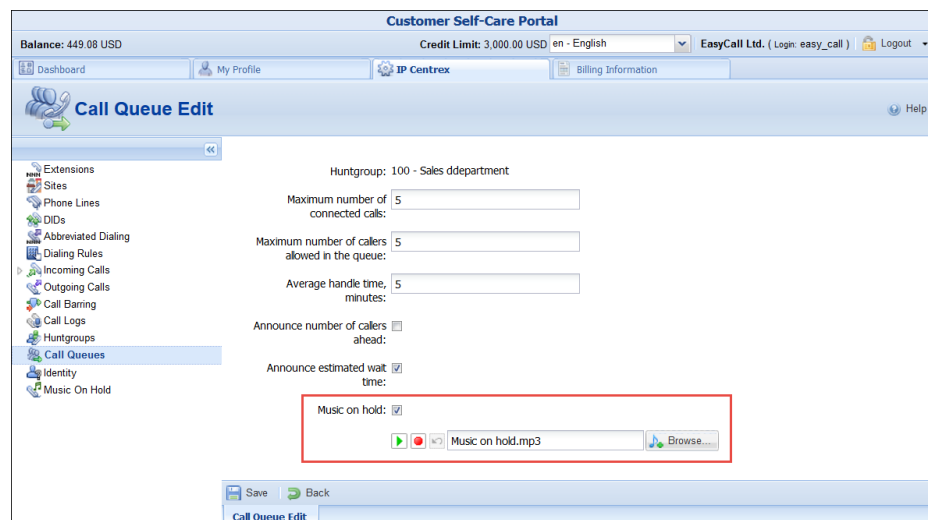
To prevent any kind of insecure connections, administrators must also enable the SSL certificates usage for connection to the call recording server (**enable_ssl** option).

When a user downloads a call record, they see the call recording server’s domain in the file download dialog window.

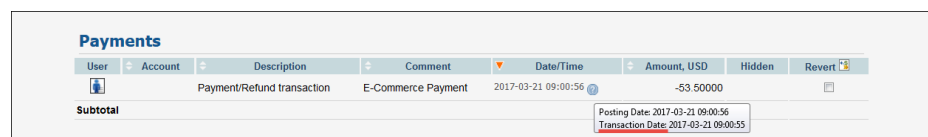
This enhancement facilitates service provisioning and ensures security for call records download.

Web Interface Changes

- **Check the music on hold prompt for call queues** – Now customers can see the name of the music on hold file they previously uploaded for call queues on their self-care interface. This keeps customers aware of which melody / announcement the caller hears when put on hold.



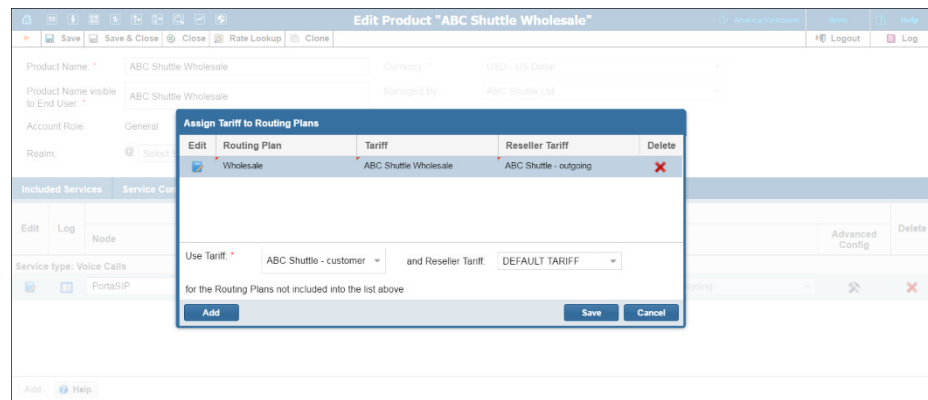
- **Renamed posted date for e-commerce payments** – The posted date is the actual date of an e-commerce transaction. With this release, to avoid confusion, the posted date for e-commerce payments on the xDR history page has been renamed **transaction date**.



This simplifies makes the web interface more user-friendly.

- **Enhanced definition of default tariffs within routing plan lists** – Now, when assigning tariffs to particular routing plans, the administrator is clearly prompted to define a default tariff that will be used for other routes (e.g. to charge users for calls that pass via their individual routing plans).

When an administrator configures a product for a reseller's use, two tariffs must be defined: one to charge customers and one to charge the reseller.



This enhancement facilitates the proper configuration for routing plan lists and enhances the user experience with PortaBilling®.

Important Upgrade Notes

- **New version of the Oracle Database** – Starting with this release, the Oracle Database has been upgraded to version 12c. This version enhances automatic data optimization, increases database security and availability, altogether resulting in better performance.

The key aspects of upgrading the Oracle Database to version 12c are as follows:

- Oracle Database version 12c can be installed after PortaSwitch® is upgraded to MR62. This enables customers to schedule their installations upgrades to a new database version. In the meantime, the previous Oracle Database 11g version will be supported up until and including the release of MR65;
- It is necessary to make sure you have enough free disk space for the upgrade. Thus, a minimum of 13Gb disk space is required for each database node.

The data migration from previous database version to a new one requires a downtime for single-site installations. Service relocation to the secondary site of a geo-redundant installation is recommended to ensure uninterrupted service provisioning for end users during the database upgrade. Please contact PortaOne Sales for geo-redundant solutions.

- **Security measures for transfer funds and airtime feature users** – With this new feature that permits the transfer of funds and airtime, the system sends a verification code that provides end users with extra verification. This code is sent either through email or an SMS and uses the information that the end user declared in their profile. To prevent fraud incidents (e.g. end user's credentials being stolen, contact information changed and funds transferred to an unknown account), the **Email** and **Alt. Phone** fields are restricted to being changed only by the end users. Thus, even if someone manages to get access to the end user's self-care interface, they will not have access to edit the **Email** and **Alt. Phone** fields as this information is read-only.

Beginning with this release, only customers may change the **Email** and **Alt. Phone** fields. However, to enable end users to change contact information on their self-care interface by themselves, an administrator may grant permission via the Access Control Lists (ACL) configuration.

The screenshot displays the 'Account Self-Care Portal' interface. At the top, it shows the user's balance (205.00 USD), language (en - English), and login details (17781235023). The main content area is titled 'General' and contains several sections:

- Personal Information:** Fields for Company Name (Smart Call, Ltd.), Mr./Ms./..., First Name (John), M.I., and Last Name (Doe).
- Address Information:** Fields for Country (UNITED STATES OF AMERICA), Address Line 1, Address Line 2, City (New York), Province/State (New York), and Postal Code (10025).
- Contact Information:** Fields for Contact (Mr. John Doe), Phone, Fax, Alt. Phone (+12125558799), Alt. Contact, and Email (johndoe@smartcall.com). Red dashed arrows point to the Alt. Phone and Email fields, indicating they are read-only.
- Other Information:** A Description field.

A 'Save' button is located at the bottom left of the form.

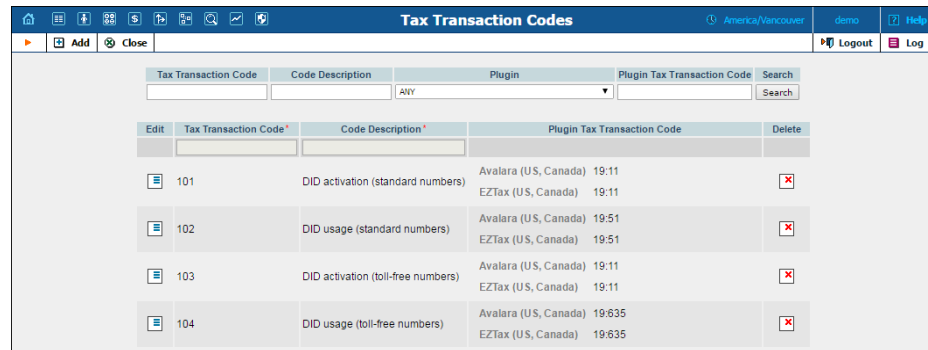
This enhancement allows service providers to protect their end users from fraud incidents.

- **Tax calculation for DID numbers via external plug-ins** – With this release, Avalara, EZtax, SureTax and GST taxation plug-ins automatically calculate taxes on DID numbers' activation and

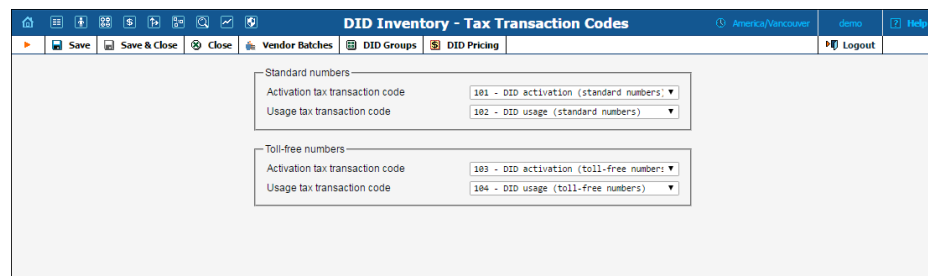
recurring charges. PortaBilling® then includes the calculated tax amounts on customers’ invoices along with other taxes.

To ensure accurate tax calculations, administrators must perform the following steps after a software upgrade:

1. Add the *internal* tax transaction codes for standard and toll-free DID numbers and then map them to the plug-ins’ tax transaction codes.



2. In the DID Inventory, define which internal tax transaction code to use for each transaction (activation and recurring).



At the end of the billing period, the taxation plug-in(s) calculate taxes for DID numbers’ charges according to the tax transaction codes defined in the DID Inventory.

- **Unified storage for SSL certificates** – SSL certificates ensure secure connection between a user’s web browser and a web server. A web server, however, can have several virtual hosts (e.g. for customized user access in different billing environments), and each virtual host requires a dedicated SSL certificate that had to be manually defined for each web instance.

To simplify certificate management, certificates are now stored on the Configuration server in `/porta_var/configurator/certs`. Upon upload by the administrator, the system recognizes the corresponding SSL certificates by their virtual hosts’ domain

names and automatically provisions them to their respective web instances when applying configurations.

Previously defined SSL certificates are moved to the Configuration server during the software upgrade.

This enhancement ensures proper system operation and reduces the administrative load.

- **New location for Sokoban external system provisioning framework (ESPF)** – For further optimization, the Sokoban ESPF has been moved to a separate `/home/provisioning_framework/` directory. If you have already configured Sokoban and created any custom event handlers, make sure to copy them from `/home/porta-admin/site_lib/Porta/Event/Handler/` to `/home/provisioning_framework/site_lib/Porta/Event/Handler/` after the software upgrade.