PORTA ONE

PortaSwitch

New Features Guide

WWW.PORTAONE.COM

Copyright Notice & Disclaimers

PortaSwitch® New Features Guide, September 2017
Maintenance Release 65
V1.65.07

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

Table of Contents

Preface

PortaSwitch® Maintenance Release 65 is the next long-life release which is mainly focused on improved system stability. It is supported with bug fixes, contains minor improvements and offers other software support for an extended period of time, thereby enabling customers to better plan the evolution of their PortaSwitch® systems.

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`.

The **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.

Bypass Menu Prompt to Dial Extension

With this release, your IP Centrex customers can enable their callers to enter a party's extension at any time once they are connected to a specific number. For instance, they can enter the extension number just after the greeting prompt or while the menu prompt is being played.

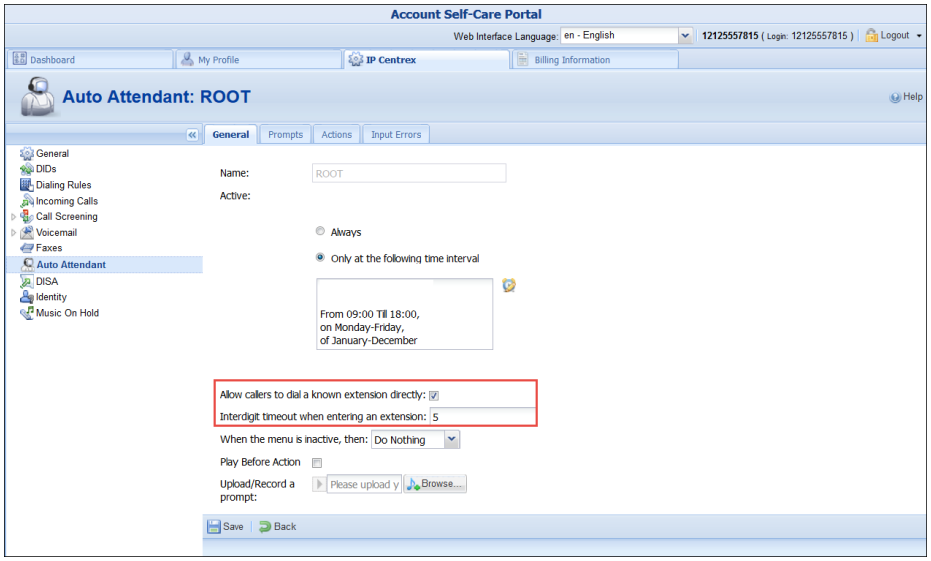
Let's say that LCGold is a small local bank where 5 bank officers work. The bank consists of two departments: Retail Banking and Loan Operations.

The bank owner wants callers to hear "Welcome to LCGold. If you know your officer's extension, please dial it. Press 1 to contact the Retail Banking department. Press 2 to contact the Loan Operations department," upon calling the bank number 12125558715.

Then, when callers dial their officer's extension, they will be immediately transferred to the officer's phone.

To satisfy the customer's requirements, an administrator creates 5 phone lines and an auto attendant with the 12125558715 number for the LCGold customer. The customer adds extensions on his web self-care interface, configures the call queues and then adjusts the auto attendant as follows:

1. On the **Auto Attendant** page of the **IP Centrex** tab opens the ROOT menu.
2. On the General tab specifies when the **ROOT** menu is active and enables the **Allow callers to dial a known extension directly** option.



3. Adjusts the **Interdigit timeout when entering an extension** option value. This is the maximum number of seconds the system waits till a user dials the second and following digits of an extension.

   This is used to define whether a user wants to enter an extension number or to select one of the menu options.

   For instance: Alice wants to reach her personal bank officer (ext. **2145**) so she calls 12125558715. Once connected, she hears the greeting and starts to enter the extension number.

   After Alice has entered the first digit (**2** in our example), the system starts the timer and waits 5 seconds for the next digit. Then:

   - If Alice does not remember the extension number and gives no input within this interval, the system considers the digit received to be a menu action and places Alice in the queue.
   - If Alice enters **1** within the next 5 seconds, the system considers the received digits to be a part of an extension number and restarts the timer. Alice enters the last two digits. If no input is received within 5 seconds, the system searches for the extension "2145"and connects the call.

   The default value for this option is 5 seconds. When changing this value, be advised that you should not slow down access to the menu actions, and should give callers enough time to enter the next extension digit.

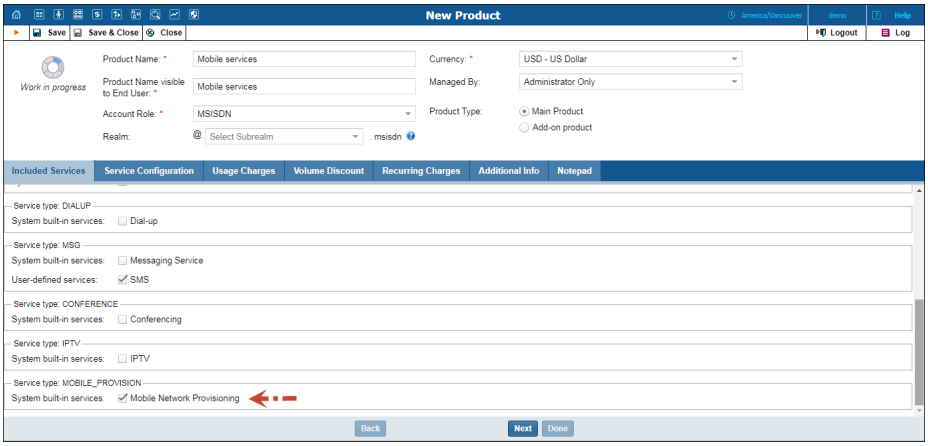
4. The customer defines the system's behavior for the period during which the menu is inactive, uploads prompts and configures actions to complete the configuration.

This feature improves the calling experience for IP Centrex customers and provides additional flexibility for system management.

Mobile Service Provisioning

To manage subscriber data provisioning to mobile networks, we introduce the **Mobile Network Provisioning** service with this release.

When the service is enabled for an account's product, the External System Provisioning Framework (Sokoban) provisions both policy / service quality parameters and account management operations accomplished in PortaBilling® to the mobile carrier's core.



This unifies the configuration procedure for different mobile service types and makes it more convenient and user friendly.

Integration with Protei HLR / HSS and Protei PCRF

In order to operate as full MVNOs / MVNEs on the mobile market, service providers often encounter a prerequisite (raised from the host MNO) to deploy such equipment as HLR / HSS and PCRF within their own networks. The joint solution developed by PortaOne, Inc. and PROTEI can easily help you meet this requirement.

PortaBilling® guarantees its integration with Protei HLR / HSS and Protei Policy Controller (PCRF) core network elements. As a provisioning system, PortaBilling® synchronizes subscriber information defined within the system with Protei HLR / HSS, and policy / service quality parameters with Protei PCRF.

To enable provisioning to Protei HLR/HSS and Protei PCRF, an administrator enables the **Mobile Network Provisioning** service for a product. For example, the administrator creates a product and configures voice calls, messaging and / or Internet access services for it. The administrator configures the corresponding service policies and enables the **Mobile Network Provisioning** service for this product. Upon assigning this product to an account with an associated SIM card, PortaBilling® provisions account and policy / service quality parameters to Protei HLR / HSS and Protei PCRF. When the administrator makes changes for an account (creating, blocking, etc.) or product, PortaBilling® immediately provisions the updated data to Protei HLR / HSS or Protei PCRF.

This integration helps service providers meet the MNO's requirements necessary to operate as full MVNOs / MVNEs. It also allows service providers to manage their subscribers and associated services independently, thereby achieving more autonomy from the host MNO.

Immediate Redirect to Call Queues

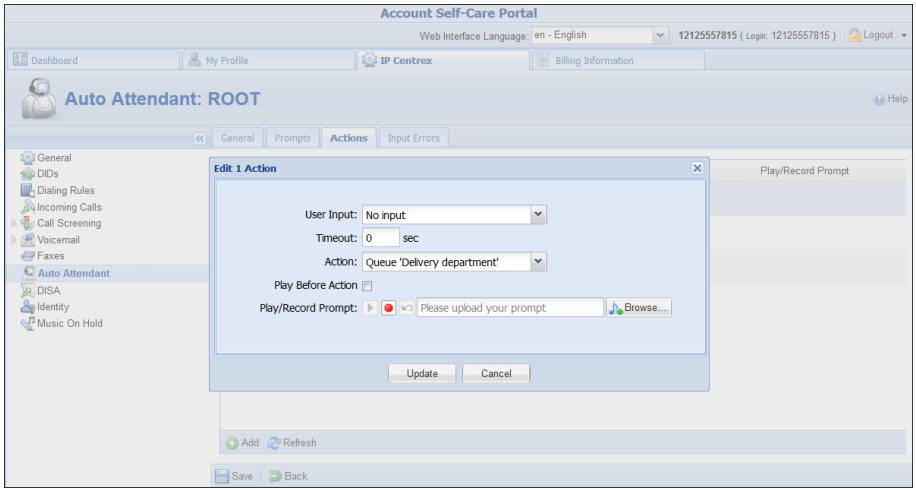
Some businesses want their customers to directly reach a specific person / department instead of listening to a long list of prompts. Now, calls that arrive to a specific number can be immediately connected to a call queue.

Let's say that David Green, a LalaPizza owner, wants his customers to order pizza delivery by calling 12125557815. Moreover, he wants to save his customers' time, so requests that his customers be directly connected to the delivery department without any timeouts.

To satisfy David's desires, your administrator creates an account with ID 12125557815 and enables the auto attendant service for it. David then configures the call queue "Delivery department" and adjusts the auto attendant configuration on his self-care interface as follows:

On the **Auto Attendant** page of the **IP Centrex** tab he adjusts the ROOT menu: specifies active periods, uploads the prompts and adds a new action using the following settings:

- **User Input** – No input
- **Timeout** – 0
- **Action** – Queue "Delivery department" and saves the settings.



Then, when Linda Roe calls 12125557815 to order a pizza, she hears "Welcome to 'LalaPizza.' You are the second person in the queue. Please wait until you are connected." While waiting she listens to music on hold.

This feature improves customer service and satisfaction and engages more customers to use your IP Centrex services.

ACL (Access Control List) Redesign

Different types of users have different responsibilities within the billing system. Some users may not be permitted to use or see certain portions of the system. To this end, PortaBilling® supports the concept of **Access Control Lists** (ACL). ACLs allow administrators to define that a particular sales representative can look at customers' data, for example, but cannot create new customers.

With this release, we are glad to present a newly redesigned and improved security system. Its main difference from the old one is that administrators use roles instead of ACLs to control user access to all of the resources in PortaBilling®. Access control lies in configuring a role and assigning this role to a user. This ensures that the user can access only those resources they are authorized to see or use.

The new security system is accessible from the new web GUI and exists in parallel with the old one. Administrators can use both new and old security systems to control user access to application resources.

Roles

Default roles are supplied with PortaBilling® – or administrators can create new roles to fit your company needs.

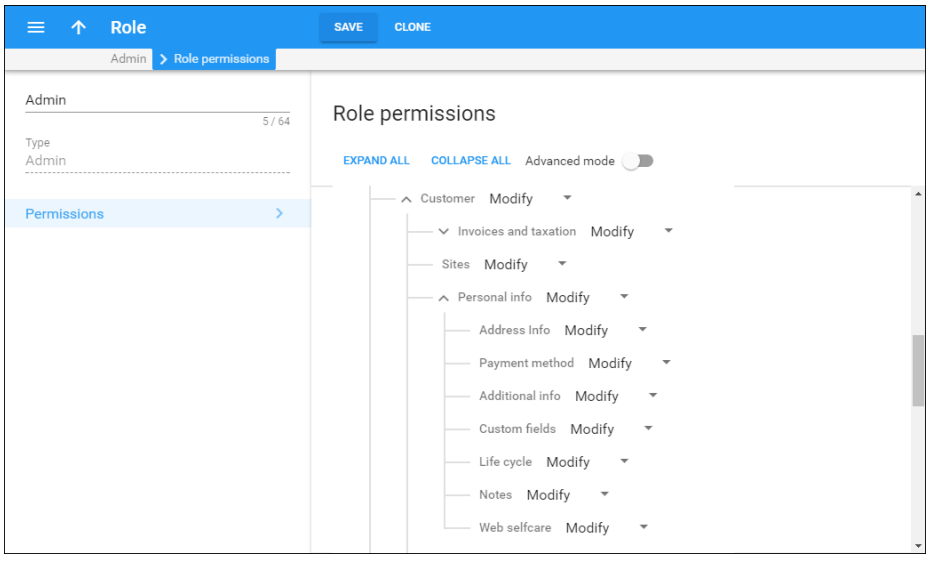
A role can be one of the following types:

- Account – to be assigned to accounts
- CC Staff – to be assigned to customer care support employees
- Customer – to be assigned to retail / reseller customers
- Distributor – to be assigned to distributors
- Representative – to be assigned to representatives
- Reseller – to be assigned to resellers
- Admin – to be assigned to users of the admin interface
- Vendor – to be assigned to your vendors

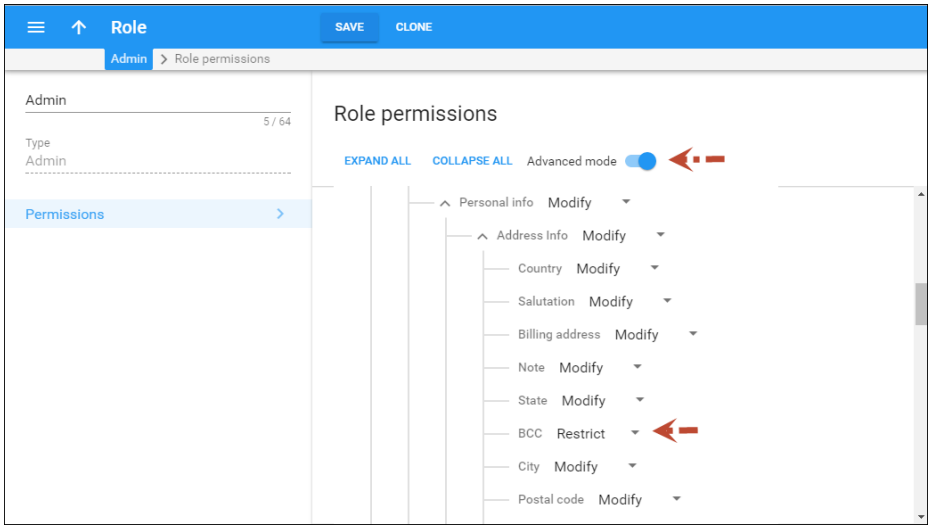
For now, only the Admin role type is available. Support for other role types will be implemented in subsequent releases.

Roles are presented on the web interface as a resource tree wherein root nodes reflect entities in PortaBilling® (i.e. customer, account, product, etc.). Second-level nodes reflect entity parameter panels. For example, for a customer entity, it can be the **Personal information** panel, **Invoices and taxation** panel, etc.

For each node within the tree, the administrator assigns permissions to define whether an entity or its parameters are available for the user and which actions the user can perform on them. The role's resource tree has a hierarchical structure, that is, lower-level nodes inherit permissions that have been assigned to higher-level nodes.



If the administrator needs to hide a certain item on an entity parameter panel (e.g. the **BCC** field on the **Address info** panel), they can switch to the **Advanced mode**. In this mode, the role's resource tree displays a list of items for each entity parameter panel. The administrator then sets the required permission for the corresponding item.



Permissions

The administrator can assign one of the following permissions in the role's resource tree:

- Restrict – This means that users cannot access the specified resource.
- Read – This permits users to view the specified resource.
- Modify – This permits users to view, update, create and delete the specified resource.

When a user attempts to perform a specific action with a resource (for example, update customer information), PortaBilling® checks whether the user has permission for this action. If permission is granted for this action, the user may proceed. Otherwise, the action is not permitted.

Two systems operating in parallel

The new and old security systems operate in parallel in the following way.

ACLs are accessible in both systems. In the new security system, administrators can assign users both roles and ACLs. However, administrators cannot see or modify ACL details.

Roles are only accessible in the new security system. In the old security system administrators can neither see / modify role details nor assign roles to users.

What happens if there is an inconsistency? For example, one administrator assigns ACL1 (or a role) to a user in the new security system and another administrator assigns ACL2 to this same user in the old

system? In this case, whatever the last changes are, are the changes that will go into effect.

This new security system makes user access management more intuitive and user friendly for administrators, thereby improving their overall experience with PortaBilling®.

Common API Entry Point for Dual-Version PortaSwitch®

Dual-version PortaSwitch® is a solution that enables service providers to perform smooth and controlled customer migration. It also provides extensible API for integration with third-party applications, CRM systems, building self-care portals, etc. Users must be able to log in to the same portal, under the same address regardless of their current location within dual-version PortaSwitch® in order to preserve their customary habits.

Thus, John Doe will log in to **www.mybilling.com** to check his balance and invoices, both when his record is on the main system and after it is moved to the new one. Administrators and resellers, in turn, must be able to operate in both systems, via the API, without reconfiguring their applications.

To this end, the API dispatcher is now introduced for dual-version PortaSwitch®. It serves as a single API entry point that unites both systems. The API dispatcher accepts API requests from applications and dispatches them within dual-version PortaSwitch® for processing. Thus, an application can receive data from the main, the new or even both systems. The decision about which data to retrieve is based on the following:

- Who uses the application – the administrator / reseller or a retail customer / account, and
- The user's location – if it is within the main or the new system.

Let's consider how retail customers and administrators / resellers operate in dual-version PortaSwitch® via the API, separately.

API for retail customers / accounts

Customers and accounts can only operate with a system where their records are located. Thus, when a customer logs on to the self-care portal, the application sends the API request to the main system. The API dispatcher checks the customer's location within dual version PortaSwitch® and if the customer was moved to the new system, it establishes the session with the new system.

Then, when the customer performs some action (e.g. selects xDRs for the previous billing period), the API dispatcher proxies the API request to the new system. The new system retrieves the xDRs and the API dispatcher delivers them to the application.

If a customer on the main system uses the self-care portal, their API requests are processed by the main system.

API for administrators and resellers

Administrators, resellers and their staff (representatives, customer care staff, etc.) manage their own configurations plus also the customers who exist within both systems in dual-version PortaSwitch®. Therefore, depending on customer location, their applications must be able to send the proper context, i.e. which system will process their requests.

For unambiguous identification of customers and accounts during the migration process, the systems in dual-version PortaSwitch® are using the shared registry for customer / account records creation. As a result, the IDs are unique across both systems so either a customer or an account is always identifiable by their ID. For detailed information and assistance in record registry configuration, contact PortaOne Support.

After an administrator has configured the interconnection between the systems, the typical workflow is the following:

- The application connects to the main system via the API and receives the session ID.
- If the application sends the API request to retrieve the customer list, the API dispatcher runs the request in both systems and merges the results within a single list. Thus, the administrator or reseller sees those customers who are still within the main system, those who were moved to the new one plus those created in the new system.
- To manage a customer from either system, the application sends the ID of this customer's record within an API request. The API dispatcher finds the system where this customer is provisioned and runs the request there. After results are received, the data is delivered to the application.
- Entities such as products, bundle promotions, volume discount plans, etc. can exist independently, i.e. not be tied to a particular customer directly. Therefore, to retrieve the list of subscriptions from the new system, the application sets the session context by providing the unique ID for the billing environment in the new system within the API request. Then the API dispatcher runs further requests within the new system.
- To operate with subscriptions from the main system, the application switches the session context by providing the ID of

the billing environment in the main system. In this case, all subsequent requests will be processed by the main system.

The API dispatcher for dual-version PortaSwitch® provides a single place for customer management and system operation and smoothes the migration process. Users preserve their habits with access to portals thereby improving their overall experience with the services you provide.

Implementation specifics

When operating with dual-version PortaSwitch® via the API, consider the following implementation specifics:

1. Applications can operate with PortaSwitch® only via the REST and SOAP API. The WebSocket API is not supported.
2. To establish a session with the new system, credentials for the API access must be the same for both systems.
3. After login, the application will be provided with the session ID that must be used in all subsequent API requests.
4. All communication between the application and PortaSwitch® is done via the main system.
5. The API dispatcher operates in conjunction with the dispatching SBC and Diameter proxy.
6. Only the get_customer_list method provides results from both systems. If you have defined limits for the list (the number of rows to retrieve), expect results that are twice as long because the same limit value will be used when querying both the main and the new system.

Known limitations

Bear in mind the following known limitations:

1. Since the application communicates only with the main system, information (e.g. its IP address) about the application on the new system is not available.
2. You can restrict access by IP address only on the main system. Since the main system connects to the new one, IP access restrictions on the new system are not considered.
3. The systems are mapped with each other by their environment IDs. Therefore, be careful when switching the environment since it may result in broken mapping and session disconnect with the new system.
4. If the main system fails to establish the API session with the new system, it operates as if there is no new system.

Dispatching SBC: Call Delivery during ZDU

One of the key advantages of site-redundant PortaSwitch® is the ability to perform zero-downtime updates (ZDU).

With this release, the dispatching SBC mediates both call and registration requests from users' devices and dispatches them to the active site for processing. Thus, users may enjoy their services without interruptions and not have to wait for their devices to re-register on the secondary site.

As soon as the update procedure begins on the main site, all services are switched to the secondary site. If a user's device from the main site sends the REGISTER request, the dispatching SBC routes it to the secondary site. The secondary site's PortaSIP® updates the device's contact information and the dispatching SBC delivers it to the device.

If a user's device has not yet re-registered with the new site during the update, the dispatching SBC keeps the NAT tunnel to this device open. Thus, if there is an incoming call to this user, the dispatching SBC sends the call request to the secondary site. Upon successful call authorization and processing, the dispatching SBC delivers the call to the user.

As soon as the main site is updated and services are switched to it again, the dispatching SBC sends all the requests from the user's devices to the main PortaSIP® for processing.

Note that secondary sites do not synchronize data with each other when operating in standalone mode. Therefore, the device can re-register on different sites during the main site's update.

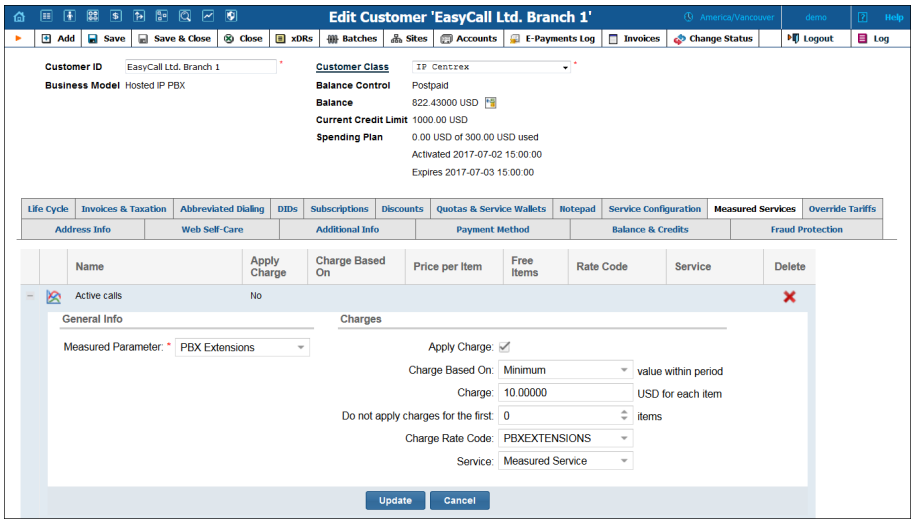
The dispatching SBC smoothes the system update in the site-redundant PortaSwitch® architecture and ensures uninterrupted service availability for users, regardless of their locations within the system.

Other Features and Enhancements

- **Charge Main and Branch Office customers individually for extensions** – Sometimes companies require their main and branch offices to be charged separately for certain services. As of now, you can charge each office for its extension usage and include those charges on their invoices.

  For example, customer EasyCall Ltd. has a main office and 2 branch offices (Branch 1 and Branch 2). Each office has several extensions: the main office has 2, Branch A has 3 and Branch B has 4.

Let's say you charge the customer $10 for each extension, and your administrator configures the measured services functionality for each office.



The main office is then charged $20. Branch A is charged $30 and Branch B is charged $40. Those charges are added to each offices' invoice at the end of the billing period.

Then let's say that the customer wants the charges for Branch A's extensions to be added to the main office's invoice and to charge Branch 2 separately for their extensions. The administrator then configures the measured services functionality for only two offices: the main one and Branch B's office.

Thus, the main office is charged $50 ($20 for its own extensions plus $30 for Branch A's extensions) and Branch 2 is charged $40. At the end of the billing period, those charges are added to the main office's and Branch B's invoices.

This enhancement provides more flexibility for billing companies with distributed infrastructure.

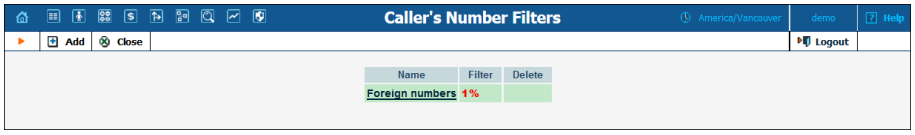
- **Extended phone number filter for call screening functionality** – Sometimes customers require that calls arriving from a group of phone numbers to be treated in a specific way. For instance, a customer wants that only calls from abroad arriving to his extension be forwarded to his cell phone in non-working hours.

To meet such needs and exclude a group of destinations from the filter list, the **Does Not Match** matching type for call screening conditions has been added.

With this release, only administrators can configure the **Does Not Match** condition for a customer on their web interface. This feature will be available for customers on the self-care portal in future releases.

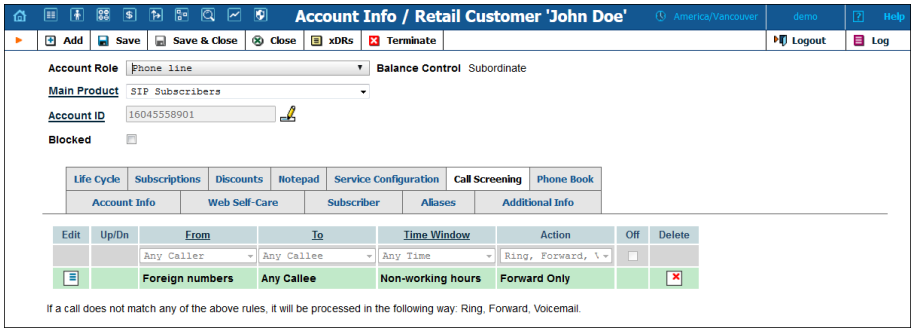
To exclude local calls from the list of numbers for the call screening rules, an administrator creates a caller's number filter with the following condition:

Foreign numbers with the **Does not match** matching type and **1%** number pattern. This assumes that the rule will be applied to calls arriving from anywhere except the USA and Canada.



NOTE: Administrators can add only one number pattern for the **Does not match** condition. The number pattern is always colored red for this matching type.

Then, the administrator configures the rules that define the system's behavior when calls arrive.

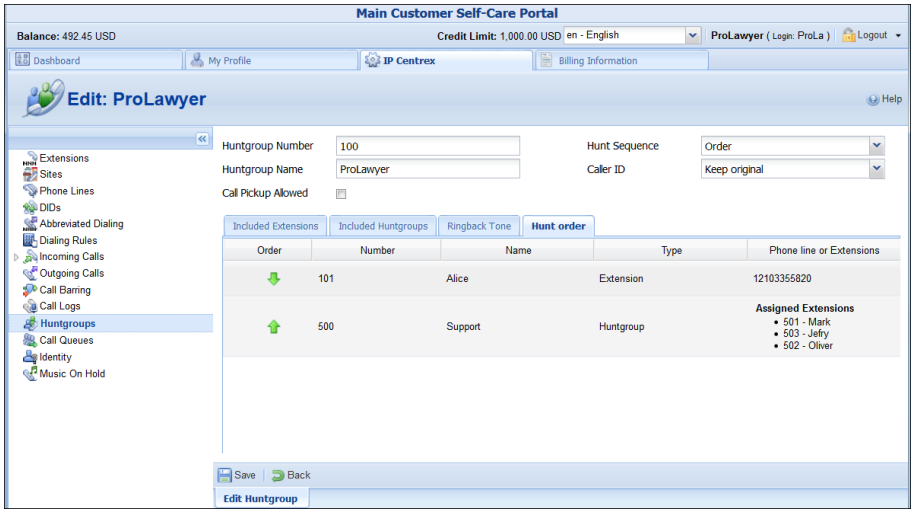


This enhancement provides more flexibility in filtering incoming calls and lessens the load on administrators.

- **Order huntgroups / extensions within a huntgroup** – Within a huntgroup, customers can now choose whether to first redirect calls to extensions or to their included huntgroups. In addition, they can now change the order of their included huntgroups.

  For example, let's say that the company ProLawyer offers legal advice and the owner wants their calls to be answered by receptionist Alice Roe. If Alice is away or unavailable, calls must be directed to the support department. The officers can clarify the purpose of the call and then transfer it to the appropriate person.

  To do that, the customer adds extensions and creates huntgroups on the customer self-care portal. Then, on the **Hunt Order** tab of the **Edit Huntgroup** page he specifies the order (Alice is 1st and huntgroup is 2nd).



NOTE: The **Hunt Order** tab only appears in huntgroups with the **Order** hunt sequence.

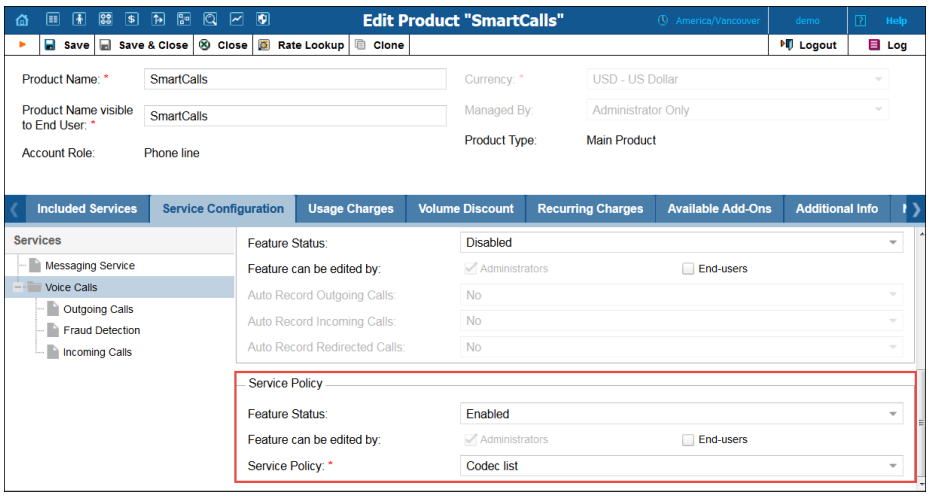
With this enhancement, ordering extensions is no longer possible from the **Included Extensions** tab.

This feature enables IP Centrex customers to perform a more flexible call distribution within their huntgroups.

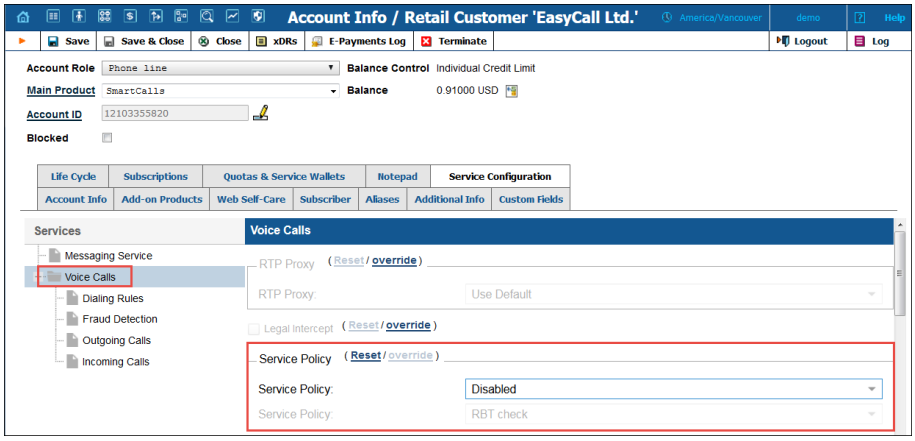
- **Enable Service Policies feature for a product** – With this release, administrators can assign a service policy to a product for voice call service. Thus, many accounts can be customized using this same product.

  Let's say you provide prepaid card services and want to lower additional costs on paid codecs (e.g. G729). You create a service policy and specify a codecs priority list within it.

Then apply this policy to many accounts by enabling it within the product and generate prepaid card accounts.



If necessary administrators can override the service policy on the account's **Service Configuration** tab.



This facilitates account management and saves administrators' time.

- **Immediate provisioning of messaging service configuration to PortaSIP®** – In the past, an administrator had to wait 60 seconds for new configuration parameters to take effect for accounts, connections, and service policies. With this release, parameters immediately update in PortaSIP® if there are any changes in the:
    - Service policy for messaging service type,
    - Vendor connection for messaging service type, or
    - Account with an account ID as an IP address.

Imagine the following example:
An administrator assigns a new product to an account – and provisioning begins immediately.

This is an enhancement that significantly saves time when provisioning a new configuration.

- **Resending of undelivered SMS messages** – When an SMS message cannot be delivered for some reason, a vendor includes an error code in the response. Previously, PortaSIP® could only receive the error codes and the message was left unsent. Now, when a code indicates a temporary error, PortaSIP® can automatically resend the SMS message.

  The first attempt to resend an SMS message occurs within 30 seconds after the error code is received and the second attempt occurs within 60 seconds. For each successive attempt, 30 seconds are added. The maximum number of attempts is 20 though you can set your own parameters in the IMGate configuration file.

  By default, PortaSIP® does not try to resend SMS messages if a vendor sends the following error codes: ESME_RINVSRCADR (invalid source address), ESME_RINVDSTADR (invalid destination address), ESME_RX_R_APPN (ESME Receiver reject message error). The other codes are considered temporary. To add more error codes that prevent SMS messages from being resent, specify these codes in the service policy for the SMPP vendor connection.

  Consider the following example:

  Lleida Networks sends an error code to indicate that their message queue is full (ESME_RMSSQFUL). Since this error code is not mentioned in their service policy, PortaSIP® attempts to resend the SMS message.

  This new enhancement helps increase the number of SMS messages delivered. Thus, service providers improve the profitability of their SMS service offerings while providing a better subscriber experience.

- **Delivery Reports for SMS Messages** – Some enterprises that organize SMS marketing campaigns require that delivery reports track the outcome of SMS message delivery. Starting with this release, PortaSIP® can send delivery reports that indicate whether or not an SMS message was successfully delivered.

PortaSIP® only provides the delivery reports by request. Thus, the enterprises must send the SMS messages with the *registered_delivery* parameter in the DELIVER_SM / SUBMIT_SM PDU.

To receive delivery reports from your vendors (to whom you send SMS traffic), configure the service policy for an SMPP vendor connection (registered_delivery = 1). Make sure that the vendors support the delivery reports beforehand. In case your vendor cannot provide delivery reports, PortaSIP® generates them on its own, based on the vendor's SMPP response message (e.g. ESME_ROK – no error, ESME_RINVDSTADR – invalid destination address).

Consider the following example:

Your customer, EasySMS, sends a bulk of SMS messages that you transfer to your wholesale provider, Lleida Networks. Once Lleida Networks provides the delivery reports, PortaSIP® transfers them to EasySMS.

The sender of the SMS messages is only charged for successfully delivered SMS messages. PortaSwitch® locks the funds required to cover the amount of the SMS messages. Once the delivery reports are received, the funds for undelivered SMS messages are unlocked.

This functionality helps service providers track delivery information about SMS messages sent. In addition, this enables them to gain new enterprises as customers, since some enterprises consider delivery reports of crucial importance.

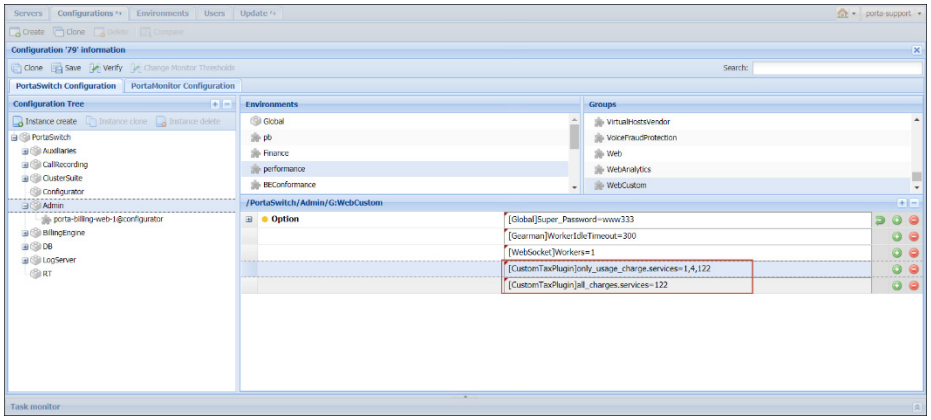
- **Override custom tax rate per service** – By default you can configure custom taxes for all charges, usage charges and recurring charges. Every type of charge has a rule that describes which services it applies to:
  - `all_charges.services=[]` – applies to charges for all services in the system;
  - `only_usage_charges.services=1,4` – applies to charges for all services **except** balance adjustments and subscriptions; and
  - `all_recurring_charges.services=4` – applies only to charges for subscriptions.

  Now you can add / exclude your custom service from specific types of charges and in this way, regulate the tax calculations for this service.

For example, let's say you provide equipment rental services (cables, fiber optics, etc.) as part of your Internet provisioning service bundle. You do not charge users for this service usage so you need to exclude it from tax calculations. To do this, you define "Equipment rental" as a separate service in PortaBilling® and mark it as not charged for usage. Then you configure custom taxes and assign them to customer classes. Lastly, you override the rules for custom tax calculations on the Configuration server web interface by adding your service's internal ID (e.g. 122) to the list of exceptions:

```
[CustomTaxPlugin]all_charges.services=122
[CustomTaxPlugin]only_usage_charge.services=1,4,122
```

where `1` and `4` are the IDs for the default services and `112` is the internal ID for your "Equipment rental" service.



NOTE: When overriding the rule you must define both the already existing services and the ones you add to the list so as to preserve their taxation.

Then when PortaBilling® calculates the taxes for your users, it skips the xDRs for the Equipment rental service.

Important! The rules for custom taxation are global for your billing environment. They apply to all custom taxes defined for a specific type of charge. Therefore, override them with caution, so as to avoid taxation misconfiguration.

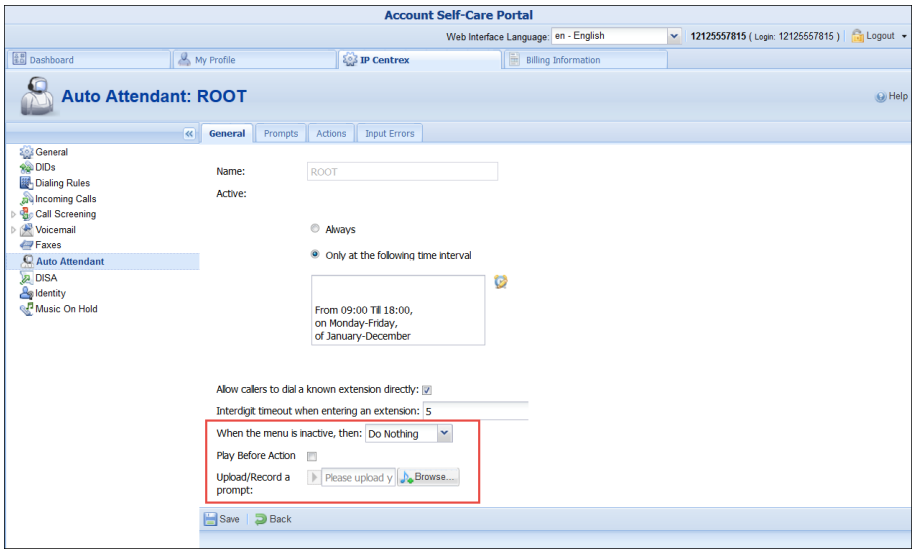
With this enhancement, you obtain advanced flexibility in applying custom taxes for the services you provide.

- **Two-phase customer migration** – To enable customers to use the services in the new system sooner, you can now transfer them without their xDRs. Then, with the second run of Porter, transfer the xDRs for these customers.

This reduces the time when customers are unable to use their services during migration.

Web Interface Changes

- **Enhanced auto attendant configuration** – Now with the ability to **immediately redirect calls to call queues** introduced in this release, the auto attendant configuration has undergone the following changes:

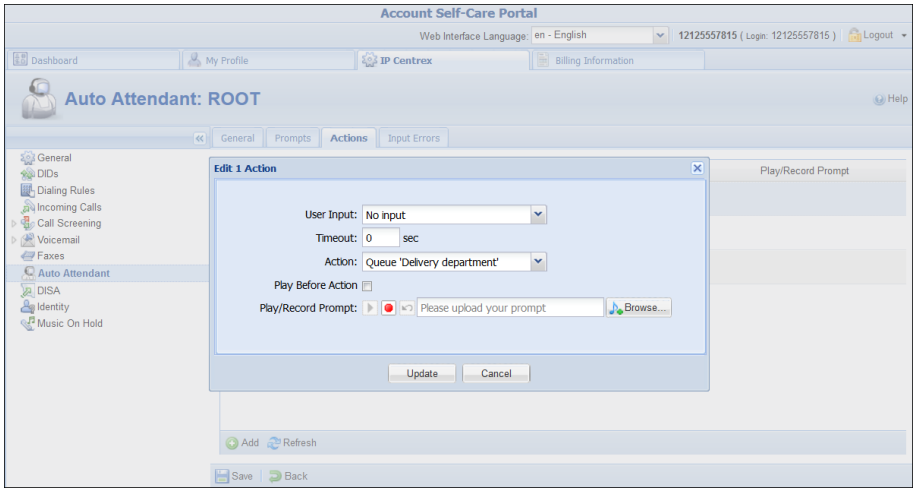


The **Not Active** user input has been replaced with the **When the menu is inactive, then** option and been moved to the **General** tab.

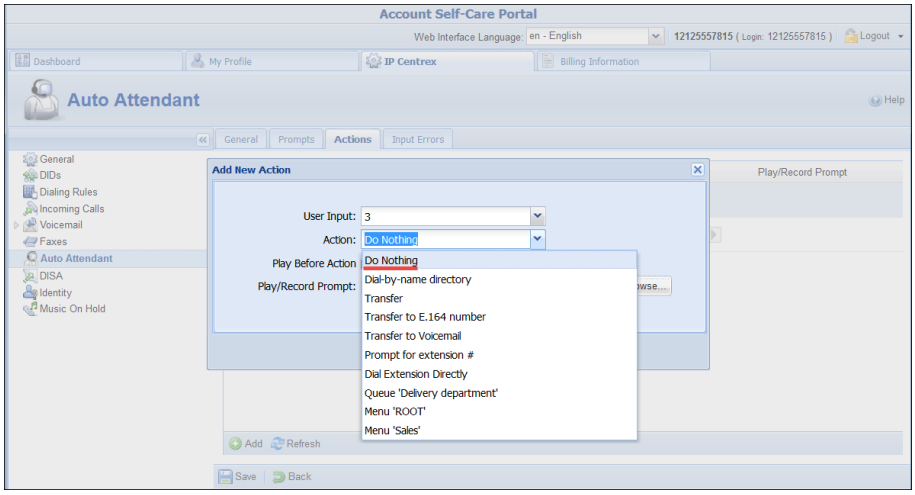
When the menu is inactive, then defines system behavior with an inactive menu. Customers can now define time periods for active and inactive menus in one place**.**

The **Timeout** user input has been renamed **No input** and been extended with the **Timeout** option.

No input assumes that users will not press any key within the time interval defined in the **Timeout** option. So if no key response is received from the caller, the system performs the defined action.

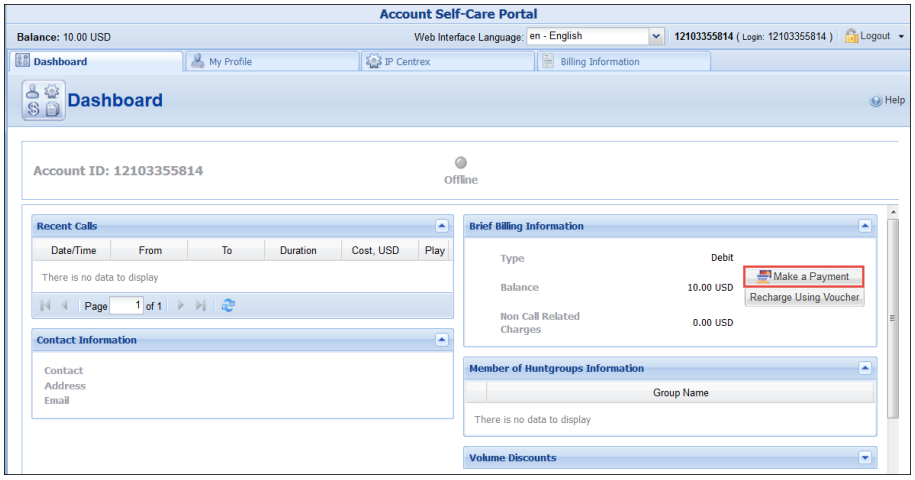


The **Disabled** action has been renamed **Do nothing.** When selected, the system does not perform any action.



These changes serve to provide advanced flexibility within the auto attendant configuration dependent upon customers' business needs.

- **The Make a Payment button has been added to the Account Brief Billing Information panel** – Now debit account owners can make payments on the **Dashboard** tab on their web self-care interface.



This simplifies e-payment procedure for end users and makes the account web self-care interface more user friendly.

Important Upgrade Notes

- **Java replaced with JavaScript applet** – Previously, the Java applet was used to let users record their greetings, prompts, etc. plus listen to different audio files via their self-care interfaces. Since the Java applet is no longer supported by Google Chrome and Mozilla Firefox, it has been replaced with the JavaScript applet.

  JavaScript doesn't require the installation of additional plugins and works in modern browsers out of the box. Therefore, users do not detect changes and are not interrupted when working with audio files on their web self-care interfaces.

- **Deprecated definition of default number translation rules** – Since PortaBilling® has built-in logic for recognizing common number modifications (e.g. numbers preceded by "+," etc.) and translates them to the E.164 format, it is no longer necessary to define such translation rules globally. Thus, as of this release, the **CLDOverrideTranslationRule** option has been deprecated and will be removed in future releases.

  If you have used such global translation rules, redefine them either as customer dialing rules or as rules for your vendor connections.