# Porta Switch®



## 25
Maintenance Release

# New Features Guide

# Copyright Notice & Disclaimers

## Table of Contents

# Preface

This document describes new features found in PortaSwitch Maintenance Release 25.

### 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`

The **exclamation mark** draws your attention to important information or actions.

**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.

## Trademarks and Copyrights

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

# 1. New Features in PortaSwitch

This section contains a description of features which involve more than one product and thus apply to PortaSwitch® as a whole.

# Improvements on the New Self-care Web Interface

PortaSwitch Maintenance Release 25 includes several enhancements in the self-care portal for end-users:

- On-demand DID provisioning enables you to offer an extensive selection of international DID numbers to your customers without any administrative overhead. The customer can pick a number belonging to the desired country/city from the inventory of DID or toll-free numbers available on the DID vendor side and then assign the number to one of his phone lines. Later the customer can easily release the number if it is not needed anymore.
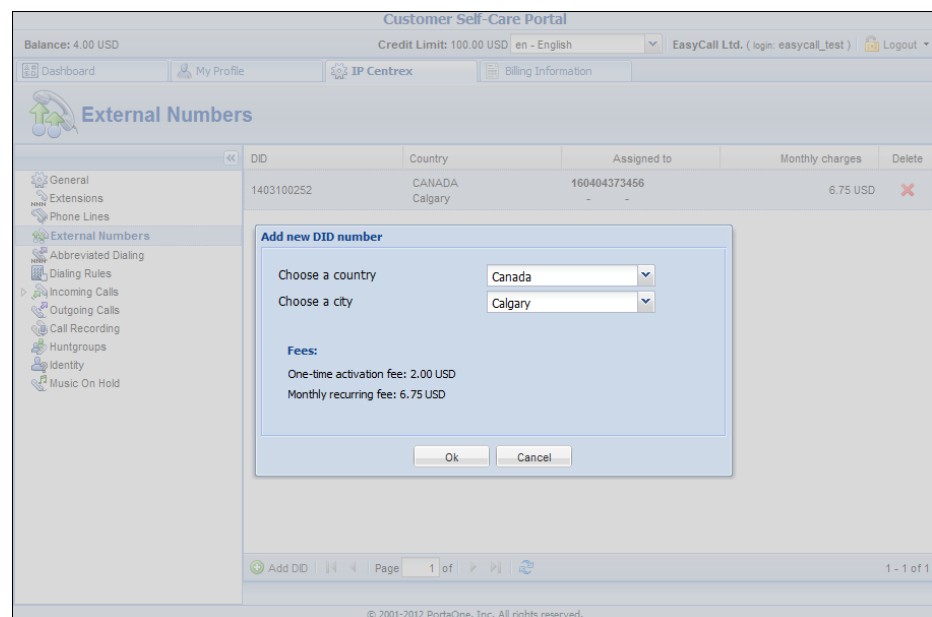


- Most important functionality for the self-care management of Unified Messaging service (which used to reside on the separate PortaUM® web portal) has been partially moved to the new self-care portal. Voice menu, faxes, external menu and greetings configurations are already available on the new self-care portal for end-user's easy and intuitive usage.
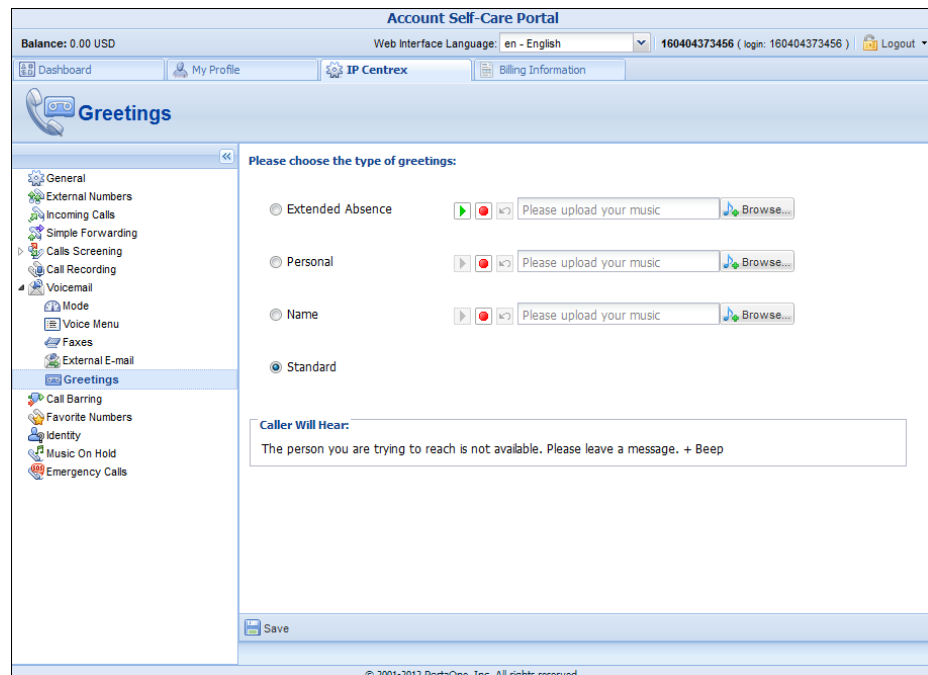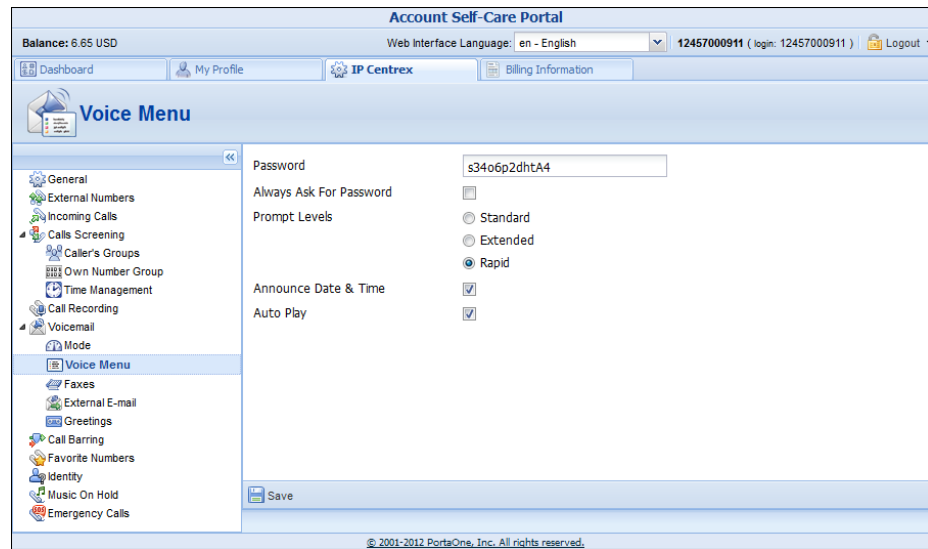
# On-demand DID Provisioning and Billing

While the traditional DID allocation method is still used when an ITSP obtains a large pool of phone numbers and then one by one, allocates numbers from it to individual customers, the appearance of "whole world a-la carte" providers such as Voxbone, DIDww or DIDx has changed the preferred way of delivering extra DID numbers from foreign countries as a value-added service. It is impractical to purchase blocks of numbers from every single country in the world in the hope that some customer is going to buy them. DID providers usually charge a monthly fee for each

allocated number, so this mode will quickly become hard to sustain financially.

On-demand DID provisioning enables the end-user to browse the complete inventory of DID or toll-free numbers available on the DID vendor side, online. When he picks a number, the sign-up process on the PortaSwitch side will reserve and allocate that number on the DID provider side and provision it inside of PortaSwitch (e.g. as an alias to an existing account). When the customer decides that he no longer needs the number (or changes the number to something else), the reverse procedure will happen – the number will be released on the DID provider side and the account/alias will be removed in PortaBilling. This allows us the ability to offer a wide variety of different DID numbers to the end-user and only be charged by the DID provider for numbers actually used by customers.
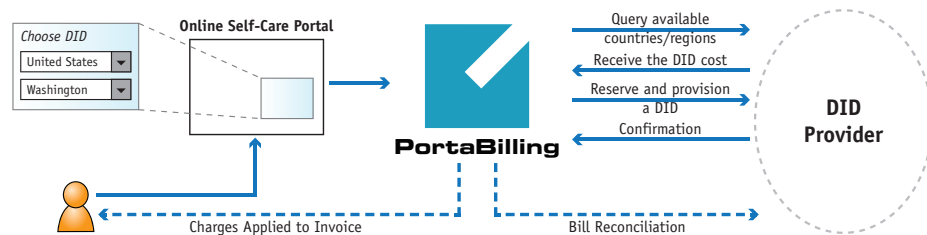


# Interconnection with DID Providers

All major DID vendors offer some type of API that can be used to query, reserve and release DID numbers. As APIs are different for different DID providers, a system of plug-in modules has been implemented (similar to those used for payment systems) that will easily allow the addition of new providers in the future.

The initial version of the DID provisioning module (part of the maintenance release 25) includes integration with DIDww (**http://www.didww.com**) provider – and more providers will be added soon based on requests from our customers.

# Number Management

The DID inventory in PortaBilling will be extended to allow ownership of a particular DID number by a specific customer. This will facilitate working with the customer's list of DID numbers, even if they are not currently assigned to any accounts. It will also allow end-customers to perform these operations via the self-care interface.

Customer and administrator will be able to see the list of the currently allocated numbers (and which extensions they are assigned to) on the "External DIDs" tab.

This approach can be used for geo and non-geo DIDs as well as for toll-free and premium numbers.

## DID Number Cost

DID providers traditionally offer DIDs on a "fixed monthly fee" basis, with no per-minute charges. The providers include access for obtaining "buying" rate information for a specific number via XML API (e.g. phone number 12065551234 will cost $5/month). This is the rate the DID provider will charge the ITSP that allocates the number to its network.

Thus, instead of trying to come up with some aggregated price list for different countries, it is possible to configure the end-user rate as a "dynamic markup" on the DID provider rate. For instance, when defining the ability to dynamically allocate US numbers from DIDww, we can specify that we would like to include a 10% markup on the DID provider rates. Thus, if a customer allocates phone number 12065551234 (DIDww rate $5/month), the end-user will be charged $5.50/month.

## DID Pricing Parameters

When defining the price to charge the end-user for a DID as a part of the DID owner information, the following parameters are available:

- **Activation Fee** is a configurable fixed amount that is charged at allocation of a new number, in addition to the DID provider's activation fee
- **Base Periodic Fee** is a configurable fixed amount that is always included in the recurring (monthly) charge
- **Percentage Periodic Markup** is a configurable increase of the DID cost (charged by the DID provider) included in the recurring charge in addition to the actual DID cost

As a result, the total charge for the DID would be:

- **At activation:** DID provider activation charge + Activation fee;
- **Monthly:** DID provider monthly charge + the markup, consisting of the Base periodic fee and the Percentage periodic markup. This formula is likely to result in some "inconvenient" numbers, such as 3.289, which are usually rounded up;

### Rounding

In order to obtain "marketable" amounts to be presented on the customer's invoice it is possible to specify the rounding pattern for the charged amounts. This will specify the last "pre-set" digits in the amount.

For instance, in a situation where number 12065551234 (which has a $1.00 activation fee and a $3.00 monthly fee charged by the DID provider) is provisioned by an end-user, the DID pricing set up would be as follows:

- $2.95 for activation markup,
- $1 for base periodic markup,
- 10% for percentage periodic markup,
- and X.99 for rounding (this parameter produces a charge amount with .99 at the end.)



The customer will then be charged $3.99 ($1.00 + $2.95 = $3.95, rounded up to $3.99) at activation and $4.99 ($3.00 + $3.00 * 10% + $1.00 = $3.00 + $0.30 + $1.00 = $4.30, rounded up to $4.99) each month.



In the case of a customer having a shorter billing period, e.g. weekly, a proportion of the DID provider's monthly fees will be used to calculate the customer's charge.

# 2. New Features in PortaBilling

# Tools for Prevention of VoIP Fraud

Maintenance Release 25 introduces a set of tools to prevent VoIP fraud, i.e. a situation where an attacker uses credentials stolen from a customer's IP PBX or end-point and sends unauthorized voice traffic to your network.

There are two main approaches for distinguishing between the activity of a legitimate user and a hacker:

- Deviation in usage patterns
- Deviation in the location from which the service is used (geo-IP)

The current version of the fraud protection module in PortaSwitch uses the location deviation method. This enables prevention of the majority of attacks without allowing a single fraudulent call to pass through, so there is zero loss for the service provider (or the customer). We plan to add real-time analysis of usage patterns in the next release, to allow even better control and proactive prevention of those rare scenarios where location analysis may not yield sufficient results.

## Geo-IP Fraud Prevention

If a hacker obtains the valid credentials of one of your customers, he can then send a call from his network using this username and password and even the identification of the SIP phone type. The only piece of information that cannot be easily changed by a hacker is his actual IP address. Although it is not always possible to determine a user's exact location (e.g. street address) from his IP address, information regarding the country and the ISP that owns the IP address (and leases it to the end-user) can be determined in the overwhelming majority of cases by using the database of IP address assignments (geo-IP database).

The key element in geo-IP fraud prevention is the assumption that, under normal circumstances, the majority of users will use your service from the same country (and the same region in that country). For instance, a VoIP user in Barcelona, Spain, connects to the Internet via DSL provided by Telefonica. Although his IP address is assigned dynamically by the ISP and may change, the "location" of that address will always point back to Spain. Even if he changes his ISP to Orange, his IP address will still refer to Spain. Usually, larger customers who use SIP trunking services are the primary target for hackers, since they have higher credit limits and are authorized to send larger numbers of simultaneous calls. By using the credentials of such a customer, a hacker can send a significant amount of traffic in a relatively short time period. Fortunately, geo-IP fraud prevention is especially accurate for this type of customer. A residential

user may take his SIP phone with him to a different country while on vacation, but it is very unlikely that a company will frequently move their office (and IP PBX) to a different country.

When launching the service, the service provider creates one or more **Country / Risk Profiles**. Each profile divides the list of all the countries in the world into three zones:

- Normal locations – A country (or countries) where users intend to use the service. Service usage is allowed without restrictions.
- Unusual – Countries where it would be unusual (but still possible) for a customer to use the service.
- Restricted (high-risk) countries – Any usage attempt from these countries will be treated as a potential security breach.

Naturally, the actual selection will depend on the area where the service provider sells the service and what type of service it is. For instance, an ITSP selling business SIP trunking services in London may define the United Kingdom as the "normal" service location, and everyplace else as restricted, since all of their customers are actually based in the UK. Another ITSP, selling residential VoIP calling via a communication client on a smart phone will define the United Kingdom, France and Spain as normal locations (since they actively advertise their product in these countries and most of their customers are there). In this case, the majority of countries in the world will be listed as "unusual." Finally, those countries from which the service provider sees an increased amount of hacking attempts will be declared "high-risk."



Next, Geo-IP Fraud Detection can be enabled in individual products, thereby allowing IP verification to be performed for all accounts, using this product. This allows you to apply Geo-IP verification to business and residential VoIP products, and skip it for other products (for backward compatibility or simply because it does not fit the business model, for instance for a service similar to Skype, where users can register and use the service anywhere in the world.

## Account Attributes

The default setting for an account is "stationary," meaning that the system expects the account to always be used in the same location. A change of

country (location) is immediately considered a potential security breach. The alternative is to mark some accounts as "roaming," in which case, the system allows for a greater number of location changes. This can be useful for customers who travel frequently and use mobile devices to communicate with clients. To reduce the amount of false alerts, a change in location will be considered acceptable in such cases. However, this will make it more difficult to detect actual fraudulent activity.

Two additional conditions may be introduced for an account:
- Screened – This means that some unusual activity has been detected for this user. An attempt to make an outgoing call will connect the user to a screening IVR, where he or she must provide additional credentials to prove that this is indeed a legitimate user.
- Quarantined – This means that after being screened, this account was unable to supply valid credentials and is still generating a large number of call attempts. In order to reduce the load on your network, all such call attempts will automatically be blocked

Every account is assigned a "default" location. An administrator may override this country selection in order to allow a legitimate user to keep using the service in a country that is otherwise considered "unsafe."
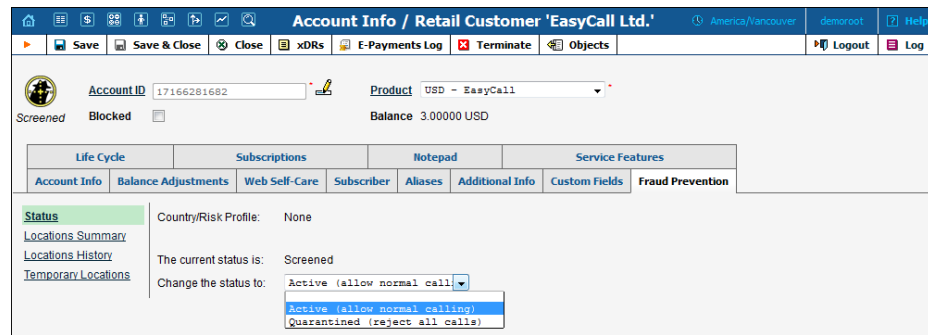


Finally, each account is assigned its own unique "service unblock" code. This is provided to the customer upon sign-up, and can be used later to confirm that a legitimate customer is attempting to make a call, therefore allowing that call from a "suspicious" location.
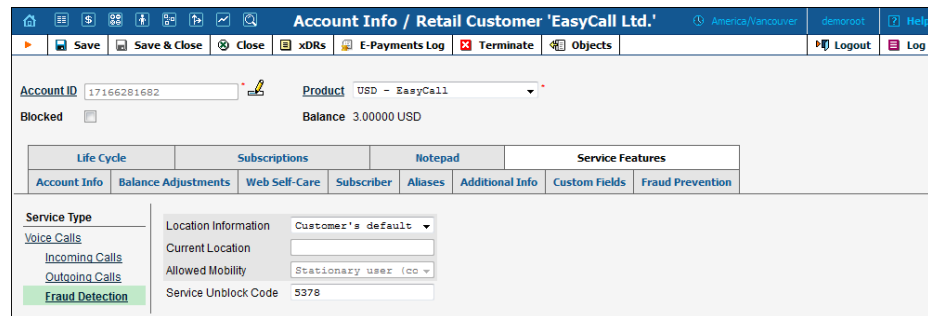
## Call Filtering

For each incoming call, the system analyzes the combination of the account's status, its default location, and the location from which the call is made.

- Any call from a quarantined account is immediately rejected.
- A call from a screened account is redirected to the screening IVR.
- If a call is made by a stationary account but the country of its current location does not match the default country, the call will be screened. If a stationary account does not yet have a default country assigned (e.g. a newly created account), the call is allowed *only* if the current country location is not on the "restricted" list.
- For roaming accounts, the call is allowed if the current country location matches the default country, or if the current country location is on the "normal" or "unusual" list.
- In all other cases, the call will be screened.

## Screening IVR

Clearly, blocking outgoing calls on any suspicion will create a negative experience for end-users. A genuine customer may take his SIP phone on an overseas trip to see his family, or a businessman may need to make a very important call while transiting an airport in an "unusual" country. The screening IVR is designed to allow legitimate customers to continue making calls in situations where their activity is considered suspicious.

- The screening IVR announces that the user's call cannot be completed because of a potential risk of unauthorized usage.
- It asks the user to re-enter the random 3-digit code he will hear. This is done to confirm that there is a live person on the line. (Hackers often use auto-dialers to test vulnerabilities in a network or generate calls to premium numbers.)
- Then the user must enter the "service unblock" code provided to him when he signed up for the service. If the unblock code is entered correctly, the system will automatically connect the user to the originally dialed number (there is no need to re-enter the number).
- If there are multiple unsuccessful attempts in the screening IVR, the account will be switched to "quarantined" status. This (along with the 3-digit "live human" verification) prevents a hacker from using a script to find the unblock code by "brute force" and continue sending traffic.

# Billing by ANI (CLI)

While calls are normally rated based on the destination number, in some situations (e.g. charging the owner of a toll-free number for incoming calls), the caller's number needs to be used to calculate the billing charges (e.g. toll-free number costs are higher if the call originates from Alaska rather than from the 48 contiguous states). This method is now fully supported, thus allowing service providers to offer a full set of incoming DID services, including toll-free DIDs.

When a call arrives to PortaSwitch from a DID vendor it is identified as coming through one of the "VoIP from vendor" connections in the system. In cases when billing by ANI (CLI) is required, an additional dedicated connection will be created. Among the "technical" parameters (such as the remote IP address) and the indication that a call should actually be charged based on ANI (CLI), this connection will also contain the access code that is used to select the applicable tariff in the product when the customer is billed. This allows for the use of one product that will contain "normal" tariffs (applied to outgoing calls when the call is billed by CLD) and "ANI-based" tariffs (applied to incoming DID calls).

## Configuration

1. Enter origination rates (e.g. 1778, 1800, 1866) with specific prices into separate vendor and customer tariffs. The most commonly used price can be set for a rate with the special destination: | (pipe). The latter will be used if there is no other, better match by the actual phone prefix.
2. For an incoming toll-free line provider, create the VoIP from the Vendor connection with the following distinctive features:
   o If the same vendor (same remote IP address or authorization username) sends you both normal (billed based on CLD (DNIS)) calls and toll-free call (billed by CLI (ANI)), then you can create a separate connection to handle toll-free calls. Specify the prefix for toll-free numbers (e.g. 1800) sent via this connection in the **CLD Prefix** field.

   Note: Prefix must be specified in the same format as that in which the vendor sends you the number, since connection matching is performed before the number translation rules are applied. If the vendor sends you 10-digit format (e.g. 8005551234) US toll-free numbers, you need to specify the prefix as 800 and then define the translation rule, which will add "1" to the number for any further rating-specific format (e.g. 800). In this case, PortaBilling will use this connection for calls that come from a particular IP address / username where CLD matches the specified prefix.

- From the **Tariff** drop-down list, select the previously created tariff with origination rates.
- Specify *Calling Number* in the **Rate Match Mode** option.
- Input an access code (e.g. INCOMING-TOLL-FREE) in the **Assign Access Code** field. The choice for the actual name of the access code is yours. Make sure that you define a Services & Rating entry that contains rates based on ANI (CLI) in the product with the same access code and tariff.



3. In the customer product's Services and Rating list, create a rating entry using the node selected for the connection with the access code INCOMING-TOLL-FREE. In the **Rate Match Mode** drop-down list choose *Calling Number*.

# Using PortaBilling for MVNO

To penetrate the mobile services market, there is no need to purchase expensive hardware, build your own tower network, or (in some cases) even get a license from the regulatory authorities. As a Mobile Virtual Network Operator (MVNO), you can utilize an existing mobile network to sell your products and bill your customers directly. PortaBilling can serve as the account management and billing platform for such an MVNO.

The mobile operator that hosts the MVNO will need to receive information about accounts and their status and deliver information about completed calls to the MVNO. Thus, there are two major aspects of the interaction between the MVNO's billing and provisioning core (PortaBilling) and that of the hosting mobile operator's network:

## Account management

When an account/customer is created by the MVNO, it should be provisioned to the HLR (Home Location Register) of the host mobile operator's system. Account blocking/unblocking, deletion, and so on should also be mapped to the mobile operator.

This is achieved by using External System Provisioning Framework (Sokoban) event mapping. When a change event occurs in PortaBilling (e.g. creation of a new account, product change, or suspension of a customer due to non-payment), it is queued and an integration plug-in is invoked. The application code inside the plug-in then delivers the information to the mobile operator's network using the required protocol (e.g. text files or XML API calls) and communication method.

Also, in some cases the Mobile Switching Center (MSC) can send authorization requests to PortaBilling for *every* separate call in order to provide balance control. In this case, before establishing a call the MSC will send a call authorization request (typically using the RADIUS protocol) to PortaBilling, and, based on the reply from PortaBilling, it will either allow or deny the call. Real-time call authorization is an important requirement for providing prepaid mobile services as an MVNO.

## Call data retrieval and processing

To process call data for an MVNO's customers, the mobile operator periodically delivers files to the MVNO containing the CDRs for all calls made by the MVNO's customers during a certain time interval. On the PortaBilling side, a regular CDR import is then performed.
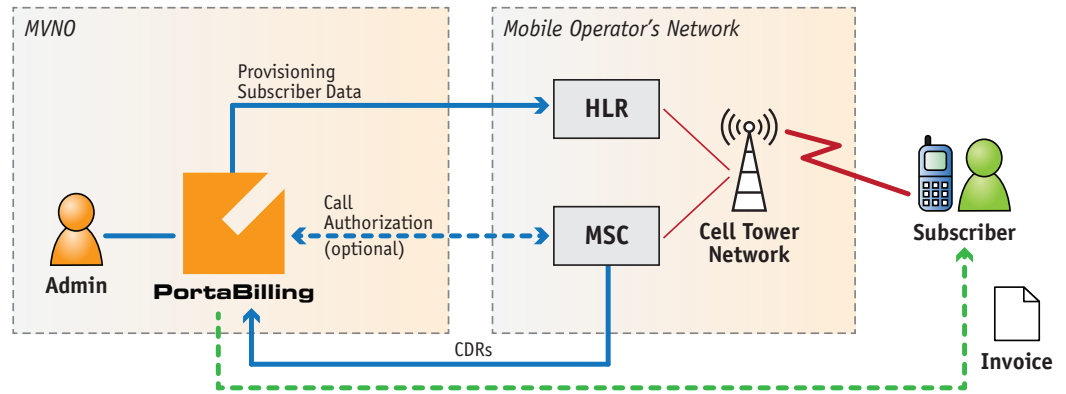
Billing customers and sending out invoices is done directly by PortaBilling, without involving the host mobile operator.

# Bandwidth-aware Limitation of Allowed Concurrent Calls

In order to guarantee a constant adequate quality of service in a situation where a customer's Internet connection has limited bandwidth, it is important to consider not only the total number of already established concurrent calls, but also how much bandwidth each one consumes. (The actual amount of bandwidth depends on the codec used and other parameters.) A new addition to the call control module allows the administrator to specify limitations in terms of the available bandwidth, so that PortaSwitch can then correctly determine whether a specific customer's site can place (or receive) additional calls.
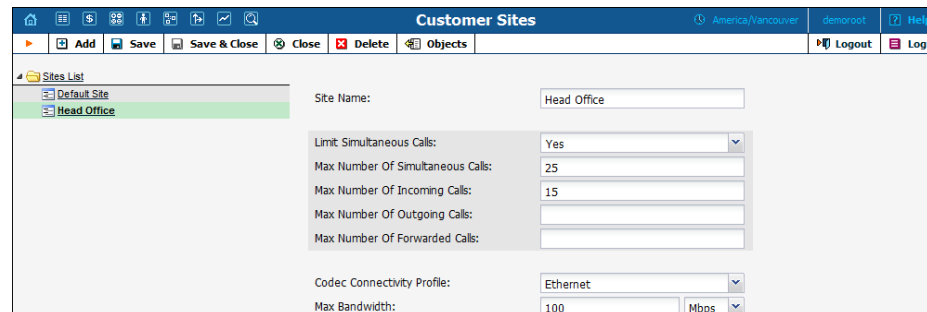


# Intra-Centrex Call Presentation

Since people normally use short extension codes to dial their colleagues, these are the numbers that they remember well. So for calls within the same IP Centrex environment, extension numbers should be visible in the call history. On the other hand, if a call is forwarded outside the IP

Centrex, the full phone number should be presented. Therefore, call detail presentation is done differently based on context. Let's look at several use cases.

## A call between two extensions

Mary Smith (extension 102) dials 101 to reach her colleague John Brown. When she (or the customer, or the administrator of the IP Centrex environment) sees the CDR, it says:

| CLI | CLD |
|-----|-----|
| 102 (Mary Smith) | 101 (John Brown) |



The same information is displayed in the incoming CDRs for this call (those viewed by John Brown).



## Calling a huntgroup

John Brown (101) dials 201 (huntgroup) to reach Sales. The CDR then shows the huntgroup number as the CLD:

| CLI | CLD |
|-----|-----|
| 101(John Brown) | 201 (Sales) |

## Using abbreviated dialing for an external number

John Brown (101) dials 401 (abbreviated dialing) to reach his partner (12065551234). The displayed CLD contains the latter's full number, as the callee is outside the Centrex environment:

| CLI | CLD |
|---|---|
| 101(John Brown) | 12065551234 |

# 3. New Features in PortaSIP

# Voiceover Announcements

Calling card services introduced many new enhancements compared to traditional home phone service, such as being able to hear your current balance, or how long you can talk for based on this balance, at the beginning of a call. Residential VoIP initially followed the traditional telephony (POTS) service model: pick up the handset, dial, get connected, talk. To make the service even better, PortaSwitch now allows the introduction of prepaid card calling features (such as announcing the maximum allowed call duration at the beginning of the call, or announcing that the call is about to be disconnected) to traditional residential VoIP service.

## Call Flow
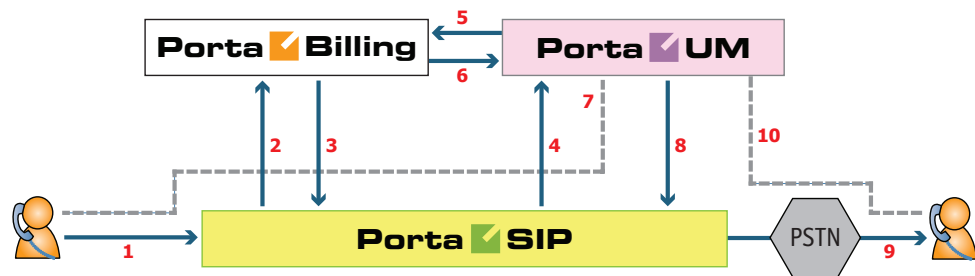


- User places an outgoing call to some destination from his IP phone, the call is received by PortaSIP (**1**) and then PortaSIP sends an authorization request to PortaBilling (**2**).
- PortaBilling determines that the call should be processed via a special IVR application on PortaUM (as opposed to sending the call directly to the destination) and informs PortaSIP that the call should be forwarded to PortaUM (**3**).
- Upon receiving a call (**4**) PortaUM launches the call control application, which sends additional authorization request to PortaBilling (**5**) and receives back the necessary information about the end-user, for instance the amount of currently available funds (**6**).
- Call control application establishes the media connection between the user's IP phone and media server, and performs required IVR actions - for instance announce the maximum allowed call duration or the current balance (**7**).
- The outgoing call is sent again to PortaSIP (**8**), where it is routed as any other outgoing call to the final destination using one of the available carriers (**9**).
- When the call is answered by the called party, the other portion of the media connection is established (**10**) and the call control application connects the caller and the callee. The media stream

still travels via PortaUM, so it can intervene at any moment – for instance to announce that the call is about to be disconnected.

# Auto-provisioning for New Models of IP Phones

Recent additions include:
- Polycom IP331
- Polycom IP335
- Polycom IP650
- Polycom IP670
- Polycom IP5000
- Polycom IP6000

# 4. New Features in PortaUM

# New Language Support

As of Maintenance Release 25, PortaUM supports Myanmar language for IVR applications such as prepaid card calling, callback and voucher balance top-up. Also the set of voice prompts for Italian language has been extended and updated.

# DISA functionality in Auto-Attendant

An extension of the existing DISA (direct Inward System Access) functionality now allows access to this function directly from the auto-attendant. For instance, an employee on a business trip who needs to make an international call can dial the company's main office line, choose the option for DISA, enter his extension number and password, and then make an outgoing call as if using his IP phone. This provides significant cost savings and improved accountability for companies who use the IP Centrex service offered by ITSPs via the PortaSwitch platform.

# Dynamic Authorization for Prepaid Card Calling

Authorization for prepaid services is usually done when a user attempts to access the service for the first time, based on the amount of funds then available. In the example of a prepaid calling card service, after the user dials the destination number his balance is converted to the maximum allowed call duration, based on the applicable per-minute rate. Since the user is authorized to use all of the remaining funds within the session (a phone call, in our example), in order to guarantee that he will not overdraw his account the system must prohibit any additional sessions while the original session is in progress. For a prepaid calling card service, this means that only one call can be made simultaneously.

In today's world converged prepaid services are becoming increasingly popular. A user with a single prepaid account (wallet) may use the funds to pay for Internet connectivity, VoIP calls, SMS messages, and so on. So it is quite possible that he will need multiple concurrent prepaid sessions (e.g. to pay for both a VoIP call and the Internet connection used for the call).

In order to allow you to provide such converged prepaid services, PortaBilling supports dynamic re-authorization, so that an external application or network node can periodically verify the available funds for a session in progress and lock the funds for the next interval.

Starting from Maintenance Release 25, the PortaUM prepaid calling card IVR is able to use the dynamic re-authorization capability of PortaBilling, so there is no need for a "one call at a time" limitation anymore - multiple calls can be made simultaneously using the same prepaid account. This also means that the customer can use additional services (e.g. send an SMS message) or add funds to the account (e.g. make a payment using a credit card) in the middle of a call, and this will alter the maximum allowed call duration.