M2M / IOT FOR CSP

PortaSwitch

New Features Guide

72

MAINTENANCE RELEASE

WWW.PORTAONE.COM

Copyright notice & disclaimers

PortaSwitch® New Features Guide, September 2018
Maintenance release 72
V1.72.08

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

PortaSwitch® Maintenance Release 72 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`.

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.

On-demand transcoding and transrating in PortaSwitch®

PortaSwitch® can now convert media stream from one codec format to another (e.g. G.711-G.729). This ensures that call parties hear each other clearly during calls and also improves the general quality of voice services.

For example, to deliver good-quality sound with limited bandwidth, you configure your customers' clients (e.g. SIP phones, mobile apps, etc.) to only use a G.729 codec. Let's say that your local telco only accepts G.711 codecs. To make the most of a low-price offer, when a call from a customer goes to the vendor, PortaSwitch® converts the media stream from G.729 into G.711 for the vendor and then back, for the customer.

Let's say that you have customers who use your voice services via satellite. For the purpose of sound quality, the media is transmitted in packets with 30 ms packetization time (the amount of voice in a single packet in milliseconds). Since your telco only accepts 20 ms, when one of these customers makes a call, PortaSwitch® then adjusts the packetization time (from 30 ms to 20 ms and back) during the call.

PortaSwitch® supports transcoding and transrating for the following codecs: G.711, G.729, G.722, G.726, DVI4, iLBC, GSM, Speex, LPC.

PortaSwitch® can support up to 1000 simultaneous conversions (e.g. G.729-G.711) per server. This number depends on the hardware capabilities of your system and which codecs you use.

Since transcoding and transrating are resource-intensive processes, they are disabled by default. Therefore, make sure to enable this feature when you update to the current version of PortaSwitch®.

With transcoding and transrating, you no longer need to think about codec compatibility between customer-premises equipment (CPE). You can choose any combination of CPEs and carriers to optimize sound quality and also minimize your termination costs.

Support of multiple early dialogs by PortaSIP® as an IMS TAS

An early dialog is the communication between call parties before a call is set up.

In IMS networks, several early dialogs can occur for the same call. These dialogs can appear because of:

- Call forking to several endpoints;
- Announcements played to the caller before a ringback tone;
- Call forwarding upon no answer.

Multiple early dialogs provide early media streams that are played to a caller. IMS equipment, including user phones, uses the P-Early-Media SIP header (RFC 5009) to identify which media stream to play:

- Carrier announcements before a call is set up (e.g. You are calling a premium number. The call cost is $2 per minute);
- Ringback tones from the called party after carrier announcements;
- Ringback tones from a remote party if the call is forwarded upon no answer.

PortaSIP® as an IMS TAS now supports multiple early dialogues and the P-Early-Media SIP header. PortaSIP® resends 183 Session Progress provisional responses from the IMS core to a caller so that their phone can select the correct media stream based on the P-Early-Media value. When a phone receives a new early dialogue with the P-Early-Media `sendonly` or `sendrcv`, it plays media from this source.

Thus, during sequential call forwarding the caller hears the announcement, “the destination is busy, please wait,” from dialog 1 and then the ringback tone from dialog 2.

This enhancement makes PortaSIP® compliant with IMS network requirements for call processing. It enables you to provide twin-card service, handle call forwarding to external networks, deliver in-band ringback tones to callers, etc.

Extended data search via the API

The `get_customer_list` API method allows filtering customer data by using attributes that are relevant to them (e.g. by customer’s home city). However, this might not be sufficient to perform advanced customer and account searches, e.g. to search for US-based customers who have spent over $100 on voice calls in a previous billing period.

The new `get_extended_data_list` API method enables you to do just that. You construct the API request and define your own search criteria as input parameters. For example, you can search for customers who live in Toronto and use the EasyCall and SuperCall products.

The API method retrieves the desired list and delivers consolidated information about customers to your CRM application. Thus, for the example above, it includes information about customers, their accounts and their products. This allows you to use PortaBilling® data via your CRM applications to execute marketing campaigns, formulate reports, etc.

The `get_extended_data_list` method is only available in JSON format. Since you create your own API requests, deeper knowledge of the PortaBilling® API is required.

Currently, the `get_extended_data_list` API method enables you to filter customers and accounts by using the attributes of such entities as:

- customers,
- accounts,
- products (both main ones and add-ons),
- customer classes and
- invoices.

Upon your request, this method can be expanded to operate using other PortaBilling® entities.

Thus, having the ability to perform an advanced data search via the API gives you the following benefits:

- The ability to retrieve data from PortaBilling® directly from your CRM or other external apps;
- Secure access to the PortaBilling® database; and
- Flexibility in forming search queries.

Integration with the Juniper MX960 Router

PortaBilling® is now integrated with the Juniper MX960 Router. ISPs use this router as a broadband remote access server (BRAS). It operates as a broadband network gateway (BNG).

With the Juniper MX960 Router you can provide high-speed (e.g. 50/100 Mbps and higher) Internet services via Ethernet cable. An administrator must first configure the router and create service policies in PortaBilling®. Then, when a user connects to the Internet, PortaBilling® authorizes them and sends their service configuration (defined in the service policy) to the Juniper MX960 via the RADIUS protocol.

PortaBilling® operates as an OCS (online charging system) for user authorization and charging. It is also used as an administrative interface for product management and bandwidth throttling (i.e. slowing and speeding). When an Internet quota is used up or expires, PortaBilling®

sends a change of authorization (CoA) request that instructs the router to change the configuration.

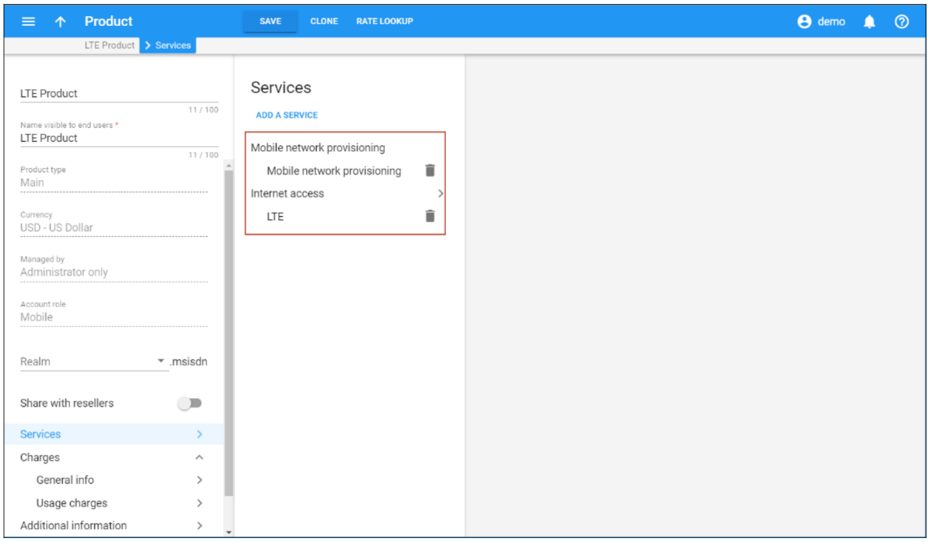
Upon request, the Juniper MX960 either reduces Internet speed and / or hotlines the user to the captive portal for replenishment. Upon payment, PortaBilling® instructs the router to resume speed.

This integration extends the variety of equipment that PortaOne's clients can use for broadband Internet service provisioning.

Integration with Adax HSS

PortaBilling® is integrated with Adax HSS – the centralized database of user subscription information. It includes user identification data (SIM card IMSI, MSISDN), user registration states, user profiles with QoS parameters and other attributes (e.g. static IP address). PortaBilling® provisions SIM card data to Adax HSS thereby enabling wireless operators to authenticate their subscribers across the LTE network and allocate the corresponding service policy to them.

To trigger Adax HSS provisioning, an administrator configures the External Systems Provisioning Framework (ESPF) and enables the **Mobile network provisioning** service within the product for LTE service.



LTE Product
11 / 100
Name visible to end users *
LTE Product
11 / 100
Product type
Main
Currency
USD - US Dollar
Managed by
Administrator only
Account role
Mobile
Realm .msisdn
Share with resellers

Mobile network provisioning
Mobile network provisioning
Internet access
LTE

Once the new subscriber account is created and a SIM card associated with it in PortaBilling®, the ESPF provisions IMSI and MSISDN to Adax HSS. Then the SIM card becomes activated in HSS and the subscriber can connect to the network.

Similarly, when an account status or service configuration changes in PortaBilling® (e.g. a SIM card is changed or additional quota is added), user data is automatically synchronized in Adax HSS.

PortaBilling® is also integrated with Adax EPC as an OCS (Online Charging System) for real-time user authorization and rating. Together, these integrations provide the ready-to-use Adax ecosystem for CSPs to organize LTE network infrastructure and provide full-scale LTE services to subscribers.

Integration with YateUCN for voice

PortaBilling® is integrated with YateUCN as the CAMEL gateway to enable CSPs to provide voice calls in 3G networks.

In this integration, YateUCN acts as the mediation component between the mobile core and PortaBilling® and also converts messages from CAMEL to Diameter Ro and back. Thus, YateUCN communicates with the mobile core via CAMEL and via Diameter Ro with PortaBilling®.

Let's have a closer look at how the call flow works:
When a user makes a call, MSC (Mobile Switching Center) performs a call authorization in PortaBilling®. MSC sends the CAMEL request to YateUCN, which converts it to a Diameter CCR-I (Credit Control Request – Initiate) message and then delivers it to PortaBilling®. Once PortaBilling® authorizes the call, YateUCN performs a reverse conversion to send the response back to MSC.

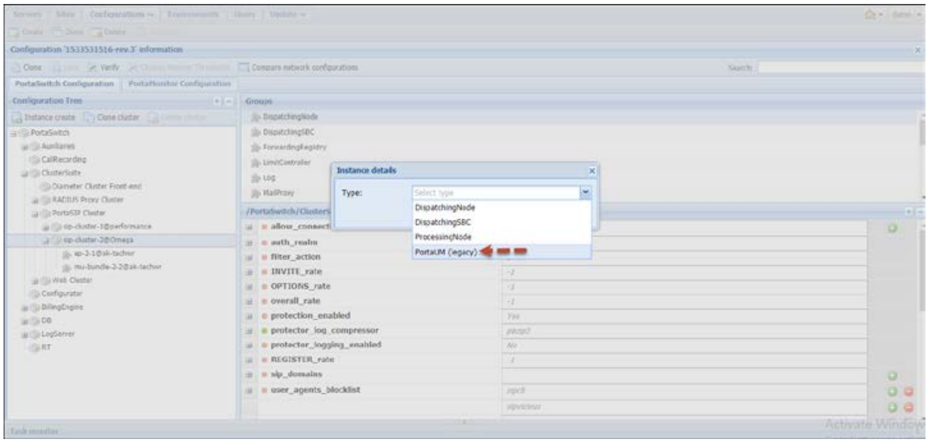
During the call, MSC sends periodic requests to update the session and lock in another portion of funds to cover the call. When the user hangs up or is left with insufficient funds to cover and continue the call, MSC sends a CCR-T request to report the end of the call. PortaBilling® then produces an xDR record and updates the user's balance. The entire communication between PortaBilling® and MSC is done using YateUCN.

YateUCN is compatible with 3G and LTE networks since it implements the functions and protocols of both core layers. PortaBilling® is already integrated with YateUCN EPC to introduce LTE services to subscribers and perform real-time billing for their usage. It is also integrated with YateHSS/HLR for SIM card provisioning (please refer to the **PortaSwitch Interoperability** guide for details).

Thus, both Yate and PortaBilling® solutions provide flexibility for organizing your network infrastructure. They also offer an opportunity to upgrade 2G and 3G network solutions to the next generation.

Dedicated media server in PortaSIP® cluster

An administrator can now allocate a dedicated media server node in the PortaSIP® cluster to handle IVR applications. This helps those customers who have legacy PortaSIP® and PortaUM® servers migrate to the PortaSIP® cluster and preserve their service provisioning flow. It also enables them to use their existing UM licenses.



When a call arrives at the access number of the calling card IVR application, the dispatching node sends the call to one of the processing nodes, which communicates with the media server node to answer the call, play IVR prompts and collect user inputs. The media server node authenticates the account (the PIN entered by the user), authorizes it for an outgoing call in PortaBilling® and communicates with the processing node to forward the call to the intended destination. The processing node sends the call to the dispatching node, which delivers it to the destination.

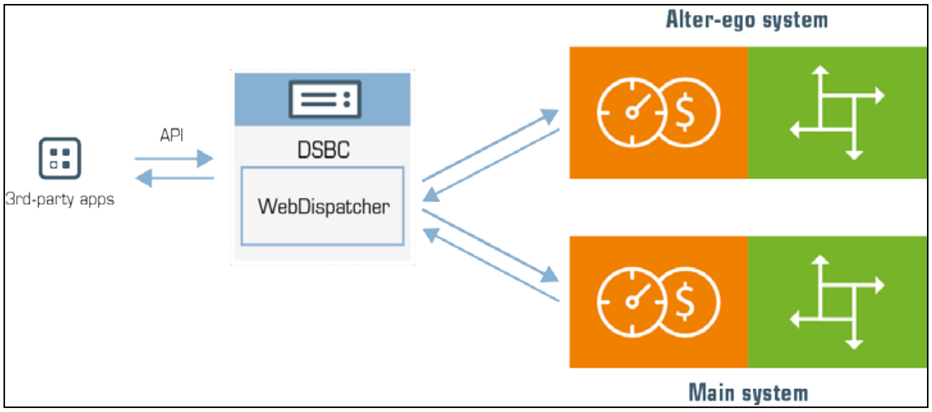
The ability to configure dedicated PortaSIP® media server nodes is also available for MR55-6 and will be added to MR60-6 and MR65-6.

DSBC: WebDispatcher

WebDispatcher for dual-version PortaSwitch® serves as a single API entry point for both the main system and the alter-ego one. It accepts API requests from applications (e.g. CRM) and number porting requests, and dispatches them across systems for processing.

With this release, WebDispatcher is one of the components of the dispatching SBC (DSBC) and operates on the same servers where the DSBC is deployed. Like other DSBC components, WebDispatcher is clustered, runs on several servers and is accessible via a single public IP address.

That is how WebDispatcher works. The application sends an API request to get customer information. WebDispatcher finds which system a customer is located in and sends a request there. After WebDispatcher receives the results, it returns that customer information to the application.



From now on, CPE profile provisioning is supported for dual-version PortaSwitch®. So when an IP phone connects to the Internet and requests a configuration file from WebDispatcher, WebDispatcher processes the request and retrieves the file from the main system, for example, and then delivers it to the IP phone.

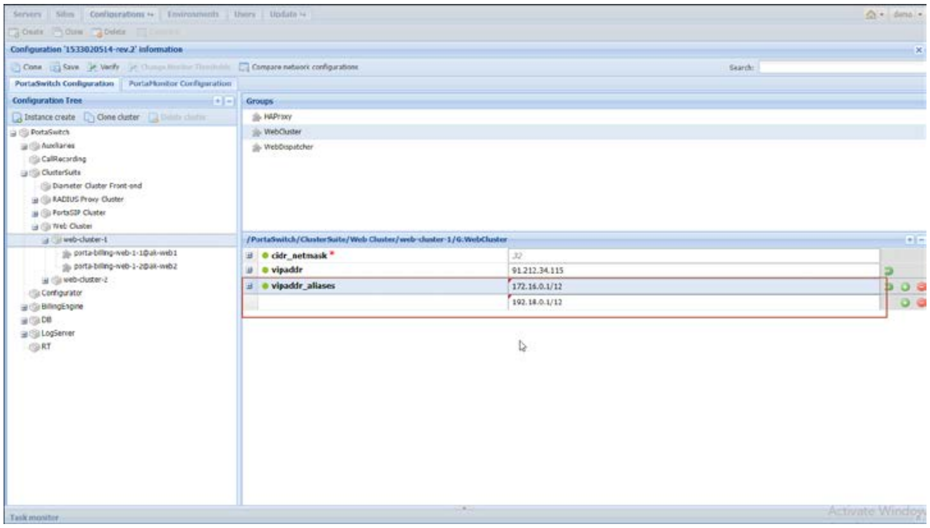
The obsolete TFTP protocol is no longer supported, therefore the HTTP protocol is supported for CPE profile provisioning in dual-version PortaSwitch®.

This feature ensures uninterrupted service provisioning during migration for your customers and makes API processing transparent.

Other features and enhancements

- **IP aliasing for web cluster** – SSL encryption is among the key requirements for websites. Encrypted sites provide a secure connection between the web server and the user, ensure the safety of user sensitive information (e.g. credentials, credit card data, etc.) and have higher rankings among search engines. In order to maintain a secure website over SSL encryption, a dedicated IP address is required.

  With this release, you can assign multiple IP addresses as aliases to your web cluster. This enables you to allocate dedicated IP addresses for your environment owners and resellers to build separate, encrypted websites.



Configuration '1533020514-rev.2' information

/PortaSwitch/ClusterSuite/Web Cluster/web-cluster-1/G:WebCluster

cidr_netmask *	32
vipaddr	91.212.34.115
vipaddr_aliases	172.16.0.1/12
	192.18.0.1/12

With a dedicated IP address, your customers and resellers can:

- Create websites under their own domain names;
- Secure the user data transmission by using their own SSL certificates; and
- Protect their websites from being blacklisted by managing the firewall configuration.

With this enhancement, you can organize white label operators to work independently. You also prevent network bottlenecks from occurring when a mass of traffic arrives at the same host and port.

- **Import CDRs in chronological order** – Now CDRs are imported and displayed on the web interface based on the exact time when a customer used a service (e.g. made a call or sent a message).

  To make this happen, the xDR Mediation utility now:
  - places source files alphanumerically before starting to import them (e.g. tata_2018-08-20_01, tata_2018-08-20_02, tata_2018-08-21_01, etc.). Thus, to process files in the correct order, please make an agreement with your vendor regarding the naming format for source CDR files;
  - sorts CDR records within a collection, chronologically, based on a time stamp. This is the time when a billing event took place (e.g. connect time for a voice call).

  To configure an xDR import in chronological order, an administrator creates **one** extracting instance and **one** rating instance. For now, it is important that only **one** rating worker process CDRs within a collection. In future releases, the option for a single CDR collection to be processed by several workers will be added.

This enhancement ensures that CDRs are rated in the order that they appear. This enhancement also provides clear service usage statistics for both the administrator and their customers in their xDR history.

- **E.164 / E.212 rate lookup for SMS services** – Now you can choose how to define rates for SMS services in customer tariffs:
    - in E.164 format, the same way you define it for voice calls, and
    - in E.212 format, as a combination of an MCC-MNC pair of codes.

  Since SMS carriers traditionally operate with an MCC-MNC pair of codes, their rates are entered in PortaBilling® using the E.212 format.

  When a user sends an SMS, PortaSIP® performs an HLR lookup to retrieve the MCC-MNC codes for the destination. PortaBilling® uses this MCC-MNC pair of codes to compute routing and calculate vendor costs.

  If a customer tariff is in an E.164 format, PortaBilling® uses the E164 rate pattern to calculate customer charges.

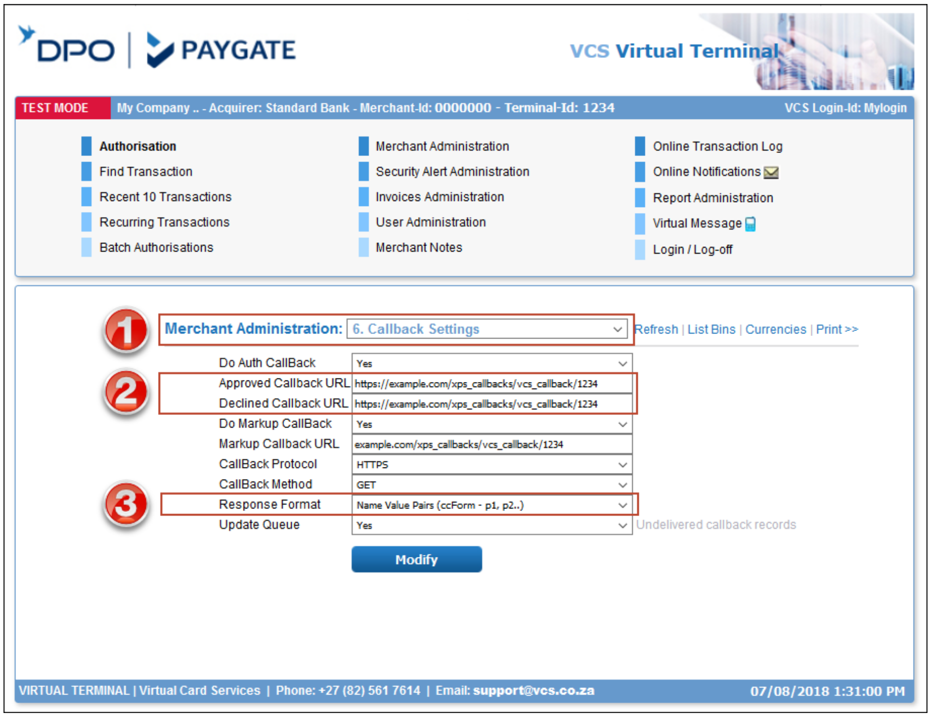
  This enhancement optimizes SMS service provisioning and allows you to:
    - Generate customer pricing in a format they can understand,
    - Manage rates, both for vendors and customers, efficiently
    - Provide clear service usage statistics to customers.

  NOTE: To properly calculate charges, reseller and customer tariffs must have the same format, either E.164 or E.212. .

- **Real-time balance updates for payments via Virtual Card Services payment processor** – The Virtual Card Services (VCS) payment processor now supports TLS v1.2. This enables the VCS to access the PortaBilling® web server and deliver transaction statuses. As a result, PortaBilling® can update customer balances as soon as their payment transactions are processed.

To enable transaction status delivery to PortaBilling®, adjust your merchant account configuration in VCS:

1. Select **Callback Settings** from the **Merchant Administration** list;
2. Define the URLs for **Approved Callback URL** and **Declined Callback URL** options in the format `https://<your_web-server_address>/xps_callbacks/vcs_callback/<your_terminal_ID>`;
3. Select the **Name Value Pairs** option from the **Response Format** list.



My Company .. - Acquirer: Standard Bank - Merchant-Id: 0000000 - Terminal-Id: 1234 VCS Login-Id: Mylogin

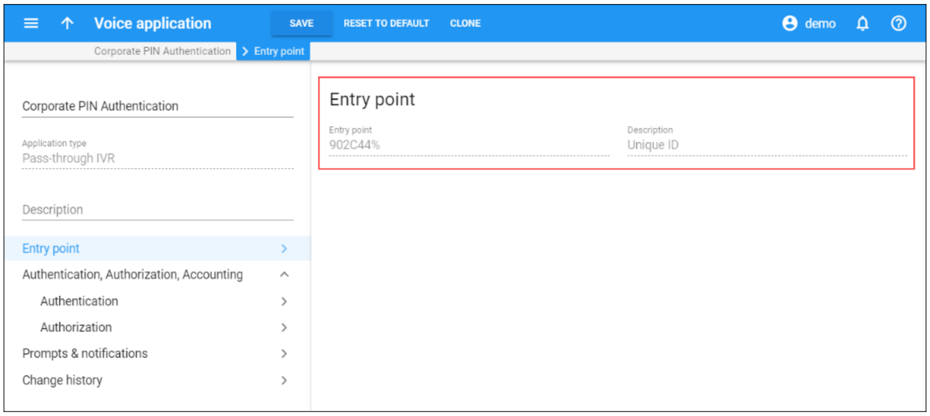
Merchant Administration: 6. Callback Settings

Do Auth CallBack	Yes
Approved Callback URL	https://example.com/xps_callbacks/vcs_callback/1234
Declined Callback URL	https://example.com/xps_callbacks/vcs_callback/1234
Do Markup CallBack	Yes
Markup Callback URL	example.com/xps_callbacks/vcs_callback/1234
CallBack Protocol	HTTPS
CallBack Method	GET
Response Format	Name Value Pairs (ccForm - p1, p2..)
Update Queue	Yes

VIRTUAL TERMINAL | Virtual Card Services | Phone: +27 (82) 561 7614 | Email: support@vcs.co.za 07/08/2018 1:31:00 PM

- **Auto generated access number for Pass-Through IVR applications –** Use the Pass-through IVR application to perform additional authorization, for example, for toll calls.

  With this release you can create a Pass-through IVR application on the new web GUI in the Voice applications section. Every Pass-through IVR application has an entry point, formerly known as access number. For security measures, the application entry point must be in non E.164 format (e.g. 5455C%). But now, when you create a new Pass-through IVR application, the system automatically generates an Entry point in non E.164 format.



Corporate PIN Authentication

Application type: Pass-through IVR

Description

Entry point

Entry point: 902C44%

Description: Unique ID

This enhancement increases the security of your system and prevents service abuse. Also, it simplifies the Pass-through IVR application configuration.

- **Denied access to self-care portal for blocked entities** – With this release, when an administrator blocks a customer or a sales agent (a distributor or a reseller), they cannot use the services nor access their self-care portal.

  For example, if you block a customer, your services (e.g. voice calls, Internet, etc.) are no longer being provided. The customer cannot log in to the portal to check or top up their balance or perform any other actions. Or, if you block a distributor, they cannot access their self-care portal to activate calling cards or enter a customer's payment into the system, etc.

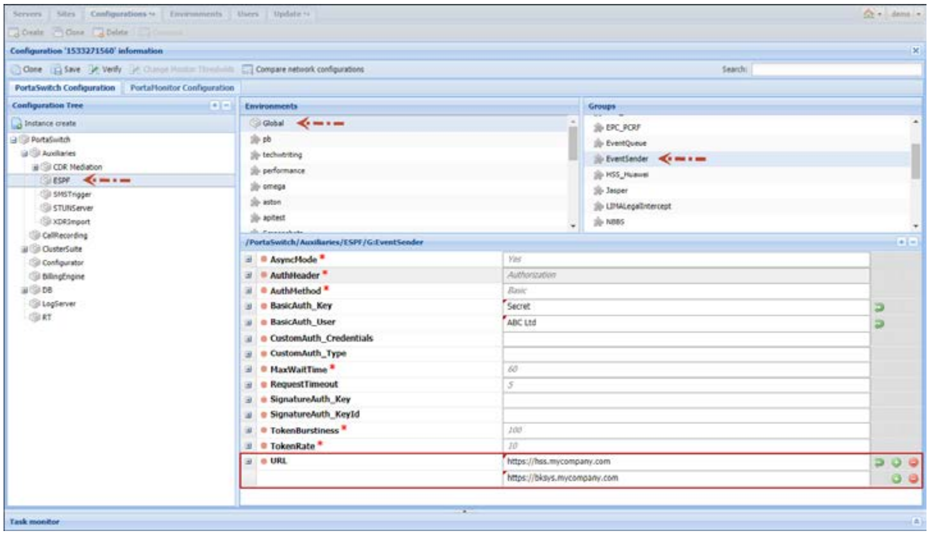
  Neither a blocked person nor their partner (a subdistributor or a subreseller) can log into the system. This prevents potential fraudulent activity (e.g. like paying their bills using a stolen credit card).

- **Simultaneous provisioning to several external systems** – The external systems provisioning framework (ESPF) can now send HTTP requests to more than one web application. This enables you to provision data to several external systems at the same time.

  Let's say that you operate as an MVNO and you provision subscriber details such as a subscriber's phone number and SIM card number to an MNO's HSS. You also provide IPTV services. Thus, when a new subscriber signs up for the service, you provision their ID and service configuration to the IPTV platform.

Since both systems use different programming interfaces (APIs), the methods for interacting with external systems differ. That is why you develop two web applications that receive requests from PortaBilling®, process them and further provision data to the HSS and IPTV platform via their APIs.

To configure provisioning to multiple destinations, an administrator adds the web applications' URL on the Configuration server.



/PortaSwitch/Auxiliaries/ESPF/G:EventSender

AsyncMode *	Yes
AuthHeader *	Authorization
AuthMethod *	Basic
BasicAuth_Key	Secret
BasicAuth_User	ABC Ltd
CustomAuth_Credentials	
CustomAuth_Type	
MaxWaitTime *	60
RequestTimeout	5
SignatureAuth_Key	
SignatureAuth_KeyId	
TokenBurstiness *	100
TokenRate *	10
URL	https://hss.mycompany.com https://bksys.mycompany.com

Note that the ESPF has a unified set of provisioning event types. This means that when a new event is detected, the ESPF sends a request to all external systems. For example, let's say that a new user, John Doe, signs up for your IPTV service.

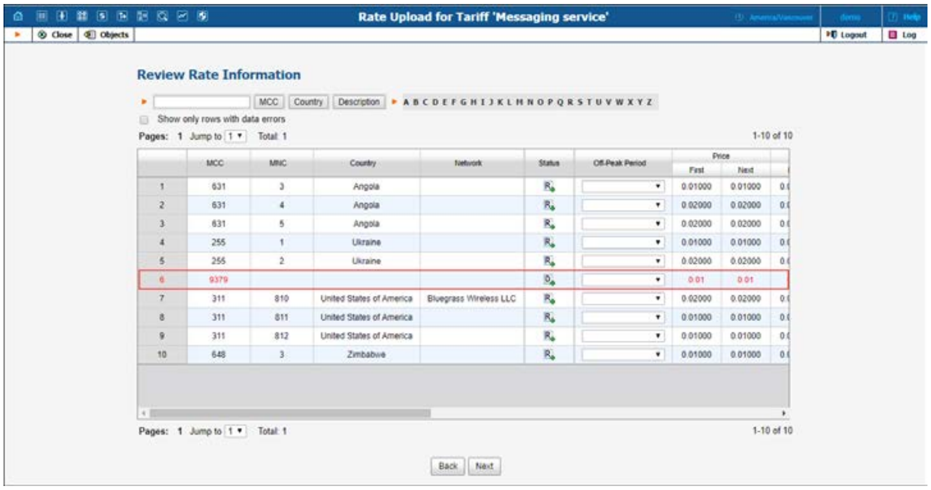
When you register John in PortaBilling®, the information is automatically sent to both HSS and IPTV platform. Since information about the SIM card is absent, it is useless for HSS. Therefore, if a service is not used by a subscriber, make sure that your web application ignores the received information.

If you wish to differentiate provisioning data and only send specific event types to each system, please contact PortaOne's support.

This enhancement makes provisioning more flexible.

Web interface changes

- **E.212 rate upload enhancements –** With this release, PortaBilling® detects incorrect rates (e.g. rates having the wrong code) and marks them in red in the Review Rate Information step. This prompts the administrator to correct the rates (e.g. by defining the proper MCC / MNC codes). If not corrected, these rates are skipped in the Create New Destination step.


Rate Upload for Tariff 'Messaging service'
Close
Objects
Logout
Log
MCC
Country
Description
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Back
Next

Review Rate Information

□ Show only rows with data errors

Pages: 1 Jump to 1 Total: 1 1-10 of 10

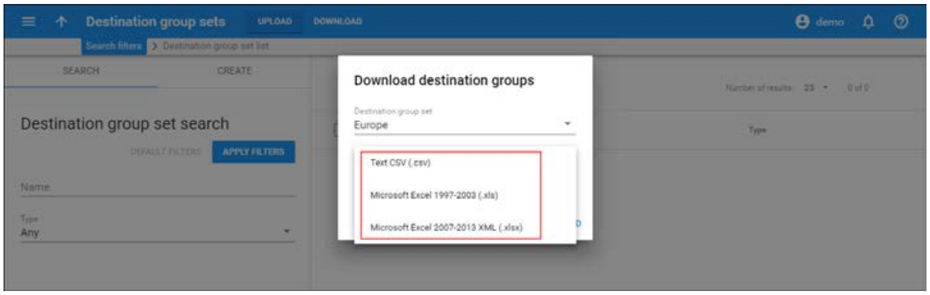
	MCC	MNC	Country	Network	Status	Off-Peak Period	Price		
							First	Next	
1	631	3	Angola				0.01000	0.01000	0.0
2	631	4	Angola				0.02000	0.02000	0.0
3	631	5	Angola				0.02000	0.02000	0.0
4	255	1	Ukraine				0.01000	0.01000	0.0
5	255	2	Ukraine				0.02000	0.02000	0.0
6	9379						0.01	0.01	
7	311	810	United States of America	Bluegrass Wireless LLC			0.02000	0.02000	0.0
8	311	811	United States of America				0.01000	0.01000	0.0
9	311	812	United States of America				0.01000	0.01000	0.0
10	648	3	Zimbabwe				0.01000	0.01000	0.0

Pages: 1 Jump to 1 Total: 1 1-10 of 10

Since there is a direct relationship between a rate MCC and its country, the country field is read only.

This enhancement ensures that rates in E.212 are uploaded correctly and improves the usability of the rate upload wizard.

- **Destination groups download file formats –** With this release you can upload and download destination groups in .csv, .xls and .xlsx formats. Thereby you work in the desired format and do not need to convert the files before upload.



Destination group set search

Name

Type
Any

Download destination groups

Destination group set
Europe

Text CSV (.csv)

Microsoft Excel 1997-2003 (.xls)

Microsoft Excel 2007-2013 XML (.xlsx)

This enhancement increases the system's usability.

- **Translation rules for node authentication removed** – In maintenance release 67, translation rules for node authentication have been discontinued. Since then, dialing rules are only configured for a single account or for a customer who owns several accounts that use the same dialing scheme.

  With this release, the Authentication translation rule option (known as Auth. Transl. Rule on the old UI) has now been removed from the administrator's web interface. If you had dialing rules configured for a node, make sure that they are now configured for your customers and / or accounts.

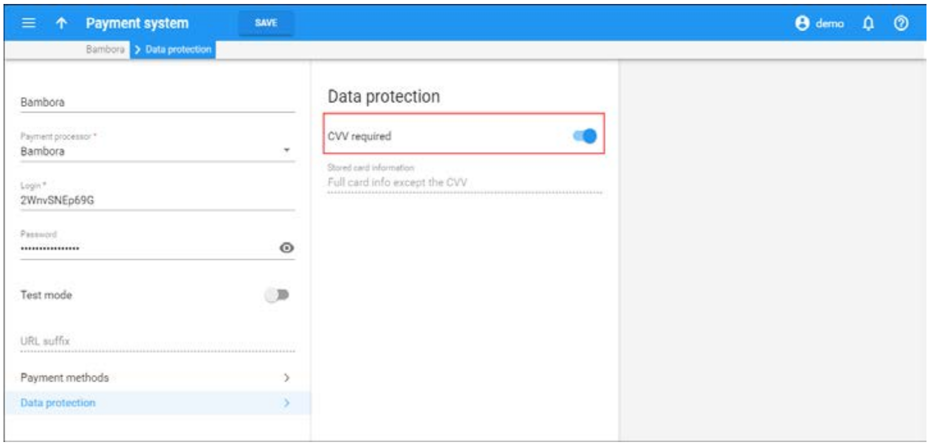
  If you use the Authentication translation rule option for additional node configuration (e.g. RADIUS Ro and Diameter Gy attributes), use service policies instead.

Important upgrade notes

- **Bambora payment processor important updates –** The Bambora (formerly Beanstream) payment processor introduces two important updates to their payment processing flow:
  - Mandatory CVV for payments
  - Switch to a new REST API

Mandatory CVV for payments

As of September 30th, 2018, the Bambora payment processor requires the CVV code to be provided for all payments. Therefore, make sure that the **CVV required** option is enabled for your Bambora payment system in PortaBilling®.



Bambora

Payment processor *
Bambora

Login *
2WnvSNEp69G

Password
••••••••••••••••

Test mode ○

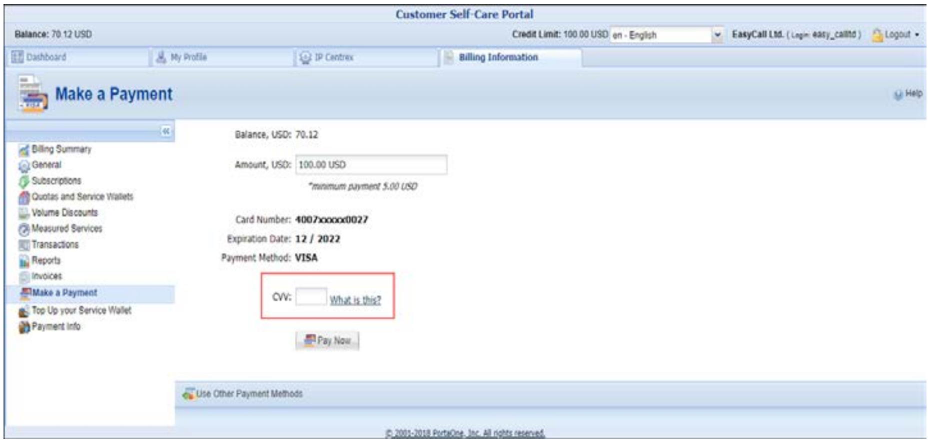
URL suffix

Data protection

CVV required ●

Stored card information
Full card info except the CVV

Since PortaBilling® does not store CVV codes, auto payments in PortaBilling® via Bambora are no longer available. Customers' credit cards remain stored in the system, but to make a payment, a customer must log in to their self-care page and enter their CVV code.



Balance, USD: 70.12

Amount, USD: 100.00 USD

*minimum payment 5.00 USD

Card Number: 4007xxxxxx0027

Expiration Date: 12 / 2022

Payment Method: VISA

CVV:

Coordinate your payment flow accordingly.

Switch to a new REST API

Bambora now uses a new REST API to process payments and PortaBilling® is fully compatible with Bambora's new REST API starting from MR70-2, MR71-1 and MR72-0.

The new REST API is incompatible with the previous SOAP API. All PortaBilling® owners who already use the Bambora payment processor must reconfigure their Bambora payment systems by performing the following steps:

- Contact Bambora support to obtain a new merchant_id and an API key.
- Specify merchant_id as a login and the API key as a password within the payment system configuration in PortaBilling®.

To simplify the migration process for their customers, Bambora supports the previous SOAP API version until 2019. After this date, it will be discontinued. Therefore, we recommend that you plan your system updates to newer releases and adjust your payment flow to meet these requirements.

- **E-commerce refunds only for payments made via the same credit card** – The e-commerce refund transaction allows you to reverse a payment transaction and credit the money from your merchant account to a customer's credit card.

With this release, you can only refund funds to the card used for making the payment. By default, this is the credit card stored for the customer in PortaBilling®; thus, e-commerce refunds are only possible to this card when done via an administrator web interface.

You can reverse payments made using another credit card via the API by specifying this card number in the request. The option to specify the card number on the e-commerce refund web interface will be added in future releases.

The same logic applies to Void and Capture payment transactions..

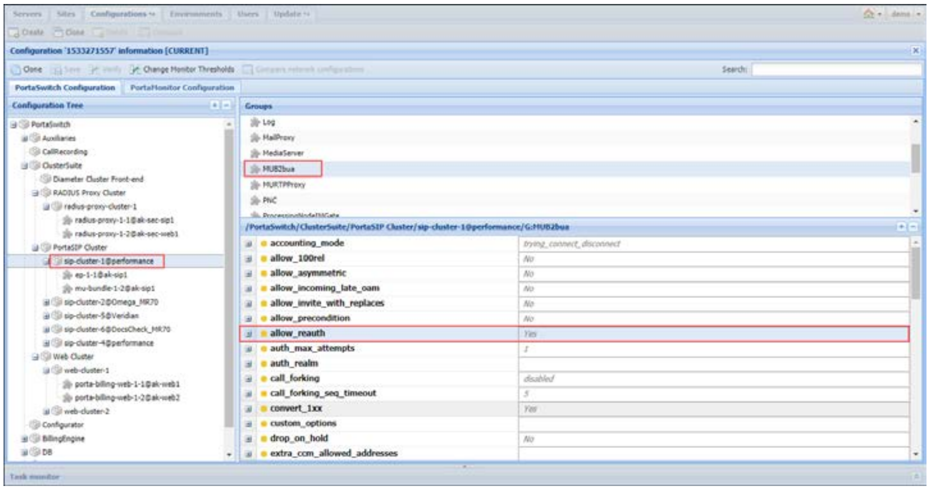
- **Unified address format for the web interface and the API** – In PortaBilling®, there are five fields in database and API structures to store address information for customers, resellers, vendors and other entities. However, on the web interface, there are only two address lines plus separate fields for city, state, country, etc. Therefore, to unify the address format in PortaBilling, the `baddr2…baddr5` fields are replaced with a single `address_line_2` field in the database and API structures.

  During a software upgrade, the values from the `baddr2…baddr5` fields are copied to the `address_line_2` field with `\n` delimiters to correctly represent them on invoices.

  For backward compatibility, `baddr` fields remain available though they are considered obsolete and will be removed from future releases. Therefore, we recommend that you use the new API field in your applications and update your invoice templates to use the `$address_line_2` variable.

- **Dynamic re-authorization is enabled by default on PortaSIP® –** Dynamic re-authorization allows customers to initiate and update concurrent sessions by locking their funds "on the go." This means that a small amount of a customer's available funds is reserved to cover each next session time interval.

Starting from MR72, dynamic re-authorization for PortaSIP® is enabled by default for new installations.



/PortaSwitch/ClusterSuite/PortaSIP Cluster/sip-cluster-1@performance/G:MUB2bua

accounting_mode	trying_connect_disconnect
allow_100rel	No
allow_asymmetric	No
allow_incoming_late_oam	No
allow_invite_with_replaces	No
allow_precondition	No
allow_reauth	Yes
auth_max_attempts	1
auth_realm	
call_forking	disabled
call_forking_seq_timeout	5
convert_1xx	Yes
custom_options	
drop_on_hold	No
extra_ccm_allowed_addresses	

When you update the system to MR72 and dynamic re-authorization is disabled, it remains disabled after the update. This is done for backward compatibility. However, we recommend that you manually enable dynamic re-authorization on the Configuration server to eliminate overdrafts.

This enhancement ensures overdraft protection for customers when they establish simultaneous sessions.