PORTA ONE

M2M / IOT FOR CSP

PortaSwitch

New Features Guide

73

MAINTENANCE RELEASE

WWW.PORTAONE.COM

Copyright notice & disclaimers

PortaSwitch® New Features Guide, October 2018
Maintenance release 73
V1.73.06

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 73 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

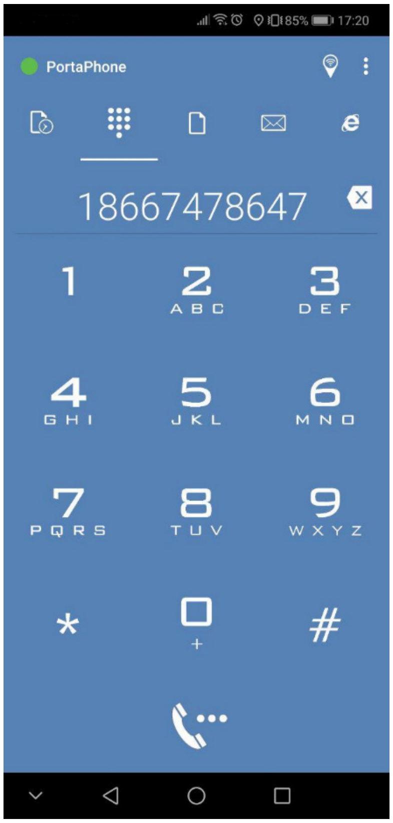
PortaBilling®, PortaSIP® and PortaSwitch® are registered trademarks of PortaOne, Inc.

PortaPhone mobile application

PortaOne introduces PortaPhone – a mobile SIP client for iOS and Android operating systems, powered by Acrobits and integrated with PortaSwitch®. You can offer it as part of your service bundle and enable users from any country to sign up for the service by using their smartphones. In this way, you quickly extend your customer base and enlarge your market share. You also save on purchasing hardware IP phones and on their delivery to end users.

PortaPhone can be branded via a dedicated web portal. You have full control over the app to customize it and publish it on Google Play under your own name. You can upload your logo, change the graphic design and manage the feature set available for customers. Thus, PortaPhone can be your private-label application.

After John Doe downloads PortaPhone from Google Play or Apple App Store, he registers his mobile phone number (e.g. 12065552453) and enters the CAPTCHA code. PortaSIP® sends an SMS with a one-time password to verify John's identity and prevent service abuse. Upon verification, John Doe can make calls and send instant messages.



PortaPhone supports voice and video calls, instant messaging, HD sound, balance checker, customizable ringtones and Bluetooth. Push notifications ensure that customers receive calls or messages while the app is in the background or even closed and use very little battery.

The IP Centrex configuration (e.g. extension dialing, call transfer, call forwarding, voicemail) is unique both for PortaPhone users and owners of IP phones. For example, if a user is not answering, the call is forwarded to voicemail or an external number. This allows your business customers to use their smartphones as their IP Centrex extensions.

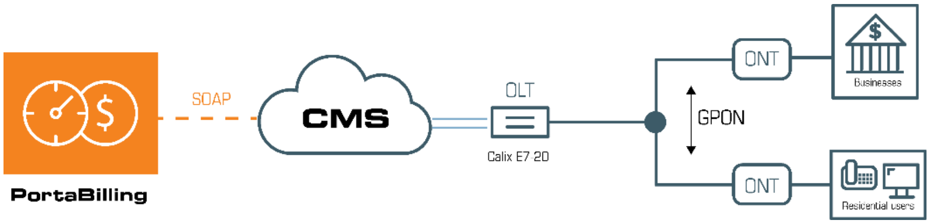
Thus with PortaSwitch® and PortaPhone you can provide services similar to WhatsApp to anyone, anywhere.

Fiber to the home service provisioning via Calix ONT

Gigabit passive optical network (GPON) and Active Ethernet (AE) are fiber access technologies that provide gigabit Internet services for subscribers. You can use them with PortaBilling® and the Calix network access equipment to deploy fiber to the home (FTTH) networks and deliver high-speed broadband Internet to your subscribers.

GPON / AE networks consist of:

- OLT – Optical Line Terminal – the service provider endpoint, and
- ONT – Optical Network Terminal – the endpoint that's located on the customer premises.



With this release, PortaBilling® provisions Calix ONTs such as:

- Calix 803G GigaPoint;
- Calix 844E GigaCenter;
- Calix 716GE-I,

and Calix E7-20 EXA Service Access Platform for GPON / AE services.

To make this happen, PortaBilling® is integrated with the Calix Management System (CMS). PortaBilling® provisions the following information to the CMS via the External Systems Provisioning Framework (ESPF):

- ONT data such as the FSAN serial number – e.g. the unique serial number of the equipment, and
- account and service configuration data, e.g. the account status, Calix bandwidth profile ID within the Internet access policy, etc.

Thus, Calix performs network access and configuration management while PortaBilling® operates as a B/OSS by providing a single place to perform customer and service management.

To provision Calix ONTs, the administrator configures the CMS by creating network uplinks for GPON services, ONT and Ethernet bandwidth profiles, etc. (Please find configuration details on the **Calix** website.)

Then the administrator configures the services in PortaBilling®, uploads the ONTs to the CPE inventory and enables the ESPF for data provisioning.

When the administrator assigns the ONT to a user's account from the CPE inventory in PortaBilling®, PortaBilling® sends the provisioning request to the CMS. The CMS activates the service for the user on the ONT and allocates the bandwidth as defined in the bandwidth profile. The user can now access the service.

When a user does not pay for their service (e.g. has insufficient funds to cover the monthly subscription fees), PortaBilling® instructs the CMS to suspend their services on the ONT until a payment is received. If the user upgrades to a new package (e.g. from 5Mbps to 20Mbps), PortaBilling® provisions the service configuration change to the CMS. The CMS allocates the new bandwidth limits on the ONT and the user receives the benefit of faster speed.

This solution enables you to build cost-effective last mile networks that work with gigabit speeds and thus meet users' increasing demands for more bandwidth. You automate the service configuration and the delivery to your users as well as its availability, based on their demands (e.g. the decision to upgrade), and their billing status (e.g. suspended upon non-payment).

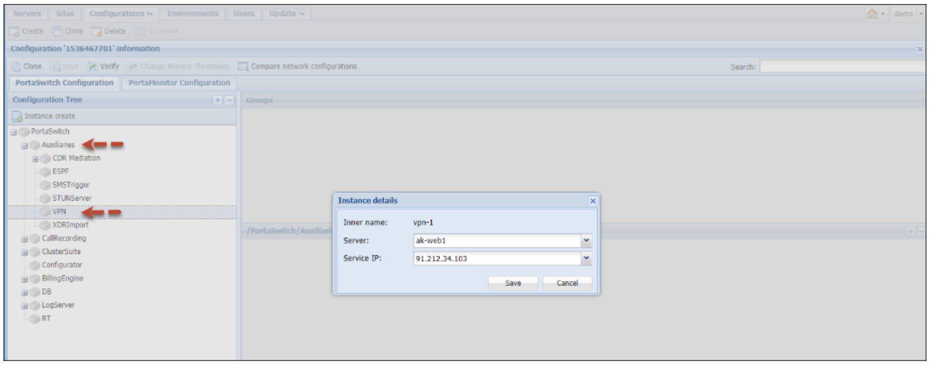
Built-in VPN solution for PortaSwitch®

In both multi-site and dual-version PortaSwitch® you must ensure that sites and systems are reachable by the Configuration server and that there is a secure channel for their communication. This means that all servers must be organized into a single virtual private network (VPN).

To save you from choosing third-party VPN equipment and to simplify VPN configuration, PortaSwitch® has a built-in VPN solution. Now you can enable a VPN endpoint on one of your PortaSwitch® servers and build secure and encrypted VPN tunnels between sites / systems.

To set up a VPN tunnel between the main and the secondary site, you must configure a VPN endpoint on every site. A VPN endpoint must have a public IP address assigned to be reachable from the outside network. The VPN endpoint's internal IP address must belong to the same subnet as the internal IP addresses of the servers of the same site.

Thus, to configure a VPN endpoint, create a VPN instance with the public IP address as its service IP.

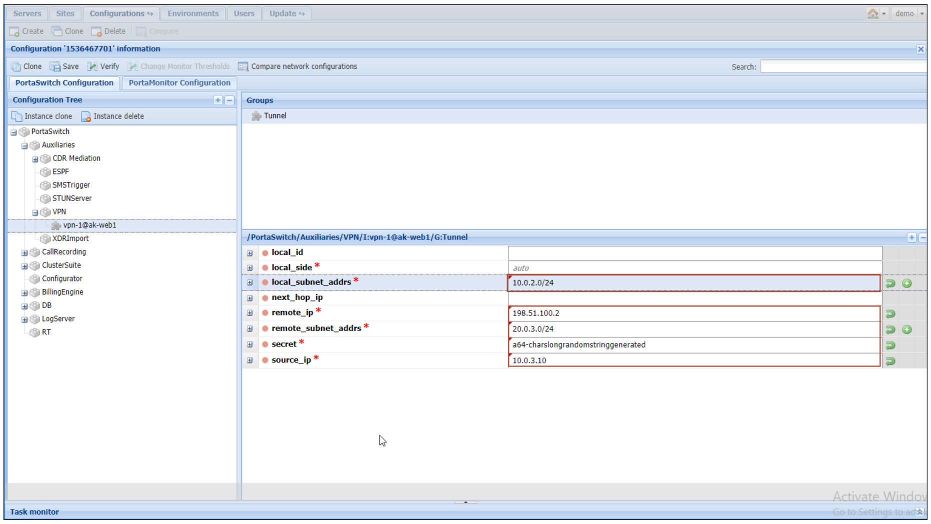


Configuration '1536467701' information

Instance details

Inner name: vpn-1
Server: ak-web1
Service IP: 91.212.34.103

Then add the local subnet, public and internal IP addresses of the remote VPN endpoint and the pre-shared key used for authentication within the instance configuration.



Configuration '1536467701' information

/PortaSwitch/Auxiliaries/VPN/I:vpn-1@ak-web1/G:Tunnel

local_id	
local_side *	auto
local_subnet_addrs *	10.0.2.0/24
next_hop_ip	
remote_ip *	198.51.100.2
remote_subnet_addrs *	20.0.3.0/24
secret *	a64-charslongrandomstringgenerated
source_ip *	10.0.3.10

You configure the VPN endpoint on the secondary site the same way. When PortaSwitch ® applies the configuration, it automatically establishes a VPN tunnel between the sites.

You can configure as many VPN instances as you need for the same site with the same service IP. For example, you can create a vpn-1 instance with IP 1.1.1.1 on the main site in New York to establish a tunnel with the fully-redundant secondary site in Canada. Then you can create a vpn-2 instance with IP 1.1.1.1 on the main site to establish a tunnel with the soft-switch based site in the UK. Note that all of the main site's VPN instances must reside on the same server.

Site-to-site VPN tunnels via NAT

Your sites can be hidden behind NAT. In this case, you can configure a VPN endpoint on a private IP address. But you must provision the public (external) and private (internal) IP addresses of the local and remote NAT routers within the VPN instance configuration.

Configure NAT routers to forward incoming UDP requests on ports 4500 and 500 to VPN endpoints. This ensures that VPN endpoints freely exchange UDP traffic.

⚠ **Important!** To avoid IP address conflicts and routing issues between VPN endpoints, the internal network addresses of your sites connected via VPN must not cross.

For detailed instructions on how to configure site-to-site VPN tunnels please refer to the **How to** section of the PortaSwitch® Configuration Server Web Reference Guide.

This solution unifies VPN configuration for all PortaSwitch® sites and simplifies network management for your administrators. It also enables you to save on purchasing third-party VPN equipment and reduces the administrative effort to maintain it.

Simple provisioning event types for new external systems

Instead of subscribing to a long list of PortaBilling® provisioning event types, external web applications can now be subscribed to a specific group such as **Subscriber**, **Customer**, **DID** and /or **Invoice**.

Events of each group notify an external web application that a corresponding entity has been **created**, **updated** or **deleted** in PortaBilling®.

Let's say that an administrator adds a new channel package for the IPTV user via an add-on product in PortaBilling®. The **Subscriber/Updated** event type that contains the unique account ID is sent to the web application. For example:

http://127.X.X.X:5000:{"event_type":"Subscriber/Updated","variables":{"i_account":1141426}}

The web application calls the `get_account_info` API method to retrieve the updated service configuration of the subscriber and then passes it to the IPTV platform. The subscriber's channel list is updated.

This enhancement enables outsource developers to quickly understand how provisioning works and to configure the application so that it properly processes incoming messages.

Other features and enhancements

- **New supported content types in PortaSIP®** – The Content-Type header defines the content type inside a SIP MESSAGE request, e.g. a text or an image.

  With this release, in addition to already supported text/plain and message/cpim content types, PortaSIP® supports these new content types:
  - **text/html** – to enable users to use HTML formatting such as bold or underlined text;
  - **application/im-iscomposing+xml** – to notify a user that their respondent is currently typing a message. The sender is not billed for sending such service messages;
  - **application/x-acro-filetransfer+json** – to enable users of Acrobits' applications to use the multimedia messaging service (*mmmsg*) that facilitates file transfer among them. Please refer to **Acrobits** for details.

  Support for these content types extends the list of IM clients that are compatible with PortaSIP®. It also extends messaging capabilities for end users and improves the user experience.

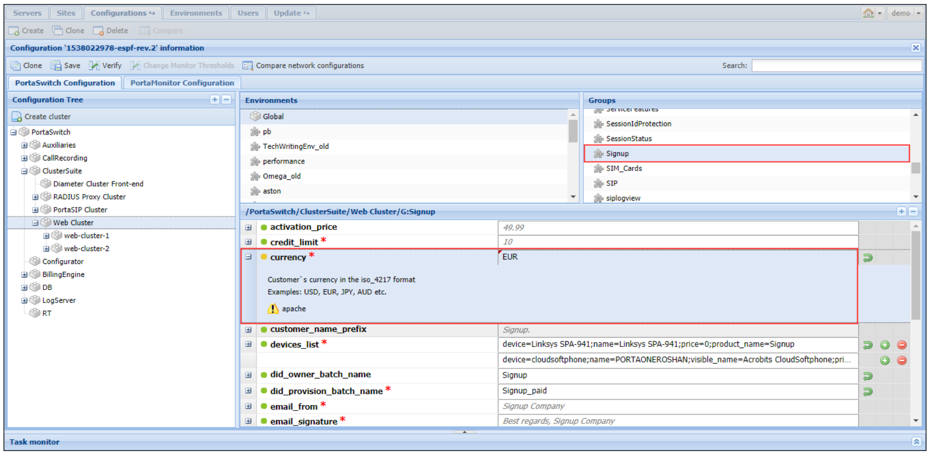
- **Improved interoperability with SMS providers** – With this release, PortaSIP® supports the transceiver / receiver mode for accepting incoming SMS messages. These communication modes are widely used for connecting with SMS aggregators (e.g. Lleida.net). PortaSIP® acts as the ESME (External Short Message

Entity) and establishes the binding connection with them that allows to receive SMS messages from the SMS aggregators.

To make this happen, an administrator configures the SMPP connection, where PortaSIP® acts as transceiver or receiver. For more details about configuration, please refer to the **Wholesale SMS Delivery** handbook.

This enhancement allows service providers to extend the list of vendors they can work with (e.g. SMS aggregators) for SMS traffic transmission.

- **Change default currency for online web signup** – Online web signup allows you to automate the process of subscribing new customers to the service. With this release, you can change a USD default currency to another one within the signup configuration by using the Configuration server. For example, if you want to create an account in EUR, you change the USD default currency to EUR. Then all the entities in PortaBilling® (e.g. products, tariffs, etc.) must also be created in EUR.



Configuration '1538022978-espf-rev.2' information

/PortaSwitch/ClusterSuite/Web Cluster/G:Signup

activation_price	49.99
credit_limit *	10
currency *	EUR
customer_name_prefix	Signup.

devices_list *	device=Linksys SPA-941;name=Linksys SPA-941;price=0;product_name=Signup
	device=cloudsoftphone;name=PORTAONEROSHAN;visible_name=Acrobits CloudSoftphone;pri...

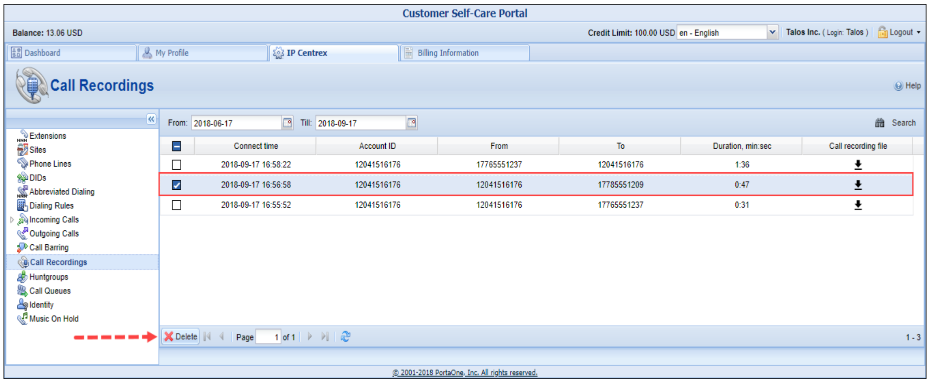
did_owner_batch_name	Signup
did_provision_batch_name *	Signup_paid
email_from *	Signup Company
email_signature *	Best regards, Signup Company

Customer`s currency in the iso_4217 format
Examples: USD, EUR, JPY, AUD etc.
⚠ apache

This enhancement simplifies signup configuration and reduces the administrative load.

- **Option of deleting call recordings** – With this release, customers can delete their call recordings via the self-care portals. Customers can decide which recordings to store or delete.

For example, let's say that EasyCall is your IP Centrex customer. Their customer, John Doe, has a call recording that contains confidential information that he wants to delete. EasyCall can delete the recording on the self-care portal. There is an option for deleting only one recording or several at one time.



Balance: 13.06 USD

Credit Limit: 100.00 USD en - English

Talos Inc. (Login: Talos)

From: 2018-06-17 Till: 2018-09-17

▬	Connect time	Account ID	From	To	Duration, min:sec	Call recording file
☐	2018-09-17 16:58:22	12041516176	17765551237	12041516176	1:36	⬇
☑	2018-09-17 16:56:58	12041516176	12041516176	17785551209	0:47	⬇
☐	2018-09-17 16:55:52	12041516176	12041516176	17765551237	0:31	⬇

Page 1 of 1

With this enhancement, an administrator provides customers with a tool to control their own personal data. Therefore, the administrator meets the GDPR requirements.

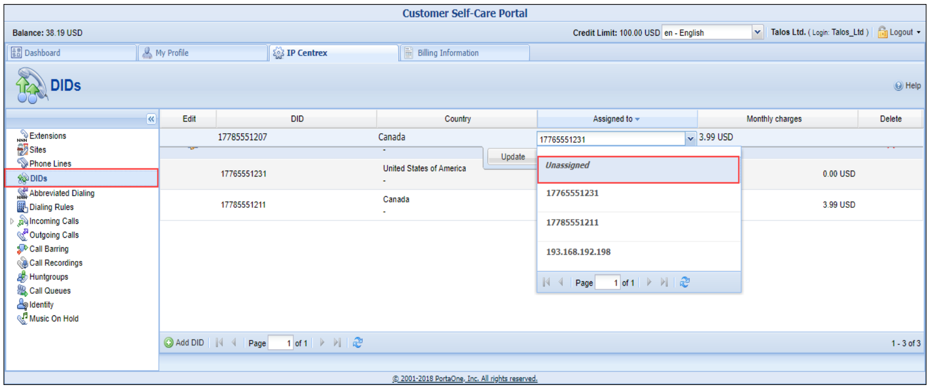
- **Preserving unique identifiers for subscriptions in dual-version PortaSwitch®** – With this release, unique subscription IDs are preserved during data migration between systems in dual-version PortaSwitch®. Thus, when you migrate a subscription with unique ID 44, for example, from the main system to the alter-ego system, its ID remains 44. This maintains a consistent workflow for API applications that use this parameter as a static value in API requests.

  The migrated subscription then remains available in both the main and the alter-ego systems. Thus, an administrator must make changes to the subscription configuration in both systems to avoid data mismatch.

  This enhancement reduces the administrative load since fewer customizations are required for API applications to make them compatible with dual-version PortaSwitch®.

- **Preserve DID for a customer when releasing it from alias** – Your IP Centrex customers can purchase a pool of DID numbers for a long period of time, e.g. for 2 years. Therefore, it is important to such customers that DIDs remain assigned to them when they manage their aliases.

  With this release, a DID number is preserved for a customer when the customer unassigns that DID number from their alias on the self-care portal. The unassigned DID can then be used to create other aliases or accounts. On the other hand, when a customer deletes their alias by clicking the Delete button, that DID number is released to the pool and is available for use by another customer.


Customer Self-Care Portal

Balance: 38.19 USD
Credit Limit: 100.00 USD
en - English
Talos Ltd. (Login: Talos_Ltd)

DIDs

Edit	DID	Country	Assigned to	Monthly charges	Delete
	17785551207	Canada	17765551231	3.99 USD	
	17765551231	United States of America -		0.00 USD	
	17785551211	Canada -		3.99 USD	

Unassigned
17765551231
17785551211
193.168.192.198

1 - 3 of 3

© 2001-2018 PortaOne, Inc. All rights reserved.

This enhancement prevents DIDs from being grabbed by another customer after alias deletion.

- **Forbidden access to the web interface for customer care staff on blocked reseller** – With this release, customer care staff that pertain to a reseller blocked by the administrator cannot access their web interface. This means that customer care staff have no power or capacity to view or process customers' personal data (e.g. name, contact details, credit card info, etc.).

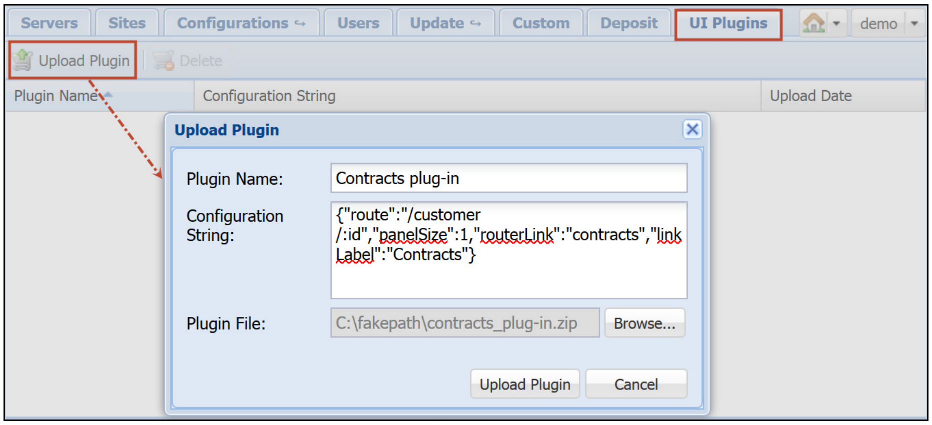
  This enhancement prevents potential data breaches and / or fraudulent activity.

- **Updated Brazilian Portuguese for IVR applications** – With this release, prompts for Brazilian Portuguese have been updated and therefore added to all Interactive Voice Response (IVR) applications such as mailbox, auto attendant, conferencing, etc.

  This enables communication service providers to offer their services in the Brazilian market or to Brazilian expats without any additional costs for localization.

- **Simplified data consolidation plug-in installation** – Plug-ins allow to integrate PortaBilling® with external systems and manage all of the data via the PortaBilling® web interface. With this release, an administrator can install a plug-in via the Configuration server instead of configuring it manually on each web server via the command line. This allows to add a plug-in one time only – and automatically have it installed on all web servers.

The plug-in data (e.g. a set of files, configuration details) is stored on the Configuration server. Thus, plug-ins are preserved after a system update to a new release. Upon adding new web servers, plug-ins are automatically installed there.



Plugin Name: Contracts plug-in

Configuration String: {"route":"/customer/:id","panelSize":1,"routerLink":"contracts","linkLabel":"Contracts"}

Plugin File: C:\fakepath\contracts_plug-in.zip

This enhancement simplifies integration plug-in installation and saves time for administrators.

Please contact the PortaOne® support team for assistance with how to install integration plug-ins.

- **Currency conversion for representative's commission** – Representatives are sales agents who sell your services for a commission. It is possible that your representatives and the customers they bring in operate in different currencies, e.g. USD and EUR. With this release, PortaBilling® automatically calculates and converts a currency for a representative's commission.

  For instance, let's say your representative Mark Johnson operates in EUR. One day he earns a $230 commission from his USD customer, so PortaBilling® converts the currency to EUR and Mark Johnson receives his €200 commission.

  This allows to identify representatives for customers with various currencies and ensures that representatives' commissions are correctly calculated and converted.

Web interface changes

- **Extended file formats for rate upload** – With this release you can upload rates in .csv, .xls and .xlsx formats. This saves you from having to convert the source files before upload.

This enhancement optimizes the rate upload procedure and thereby reduces the administrative load.

Important upgrade notes

- **Enhanced verification of service passwords** – With this release, PortaBilling® always verifies an account's service password. If the service password supplied by NAS does not match, PortaBilling® rejects the authorization request.

  There are cases when a user must be authenticated without a service password (e.g. ANI authentication). PortaSIP® instructs PortaBilling® to skip the password verification check and PortaBilling® authenticates the user by using the User-Name attribute only. No action is required from you.

  If you use a legacy media gateway (e.g. Cisco AS5300 / 5350) with an access application that requires service passwords to be ignored, configure the gateway to send the `h323-ivr-out=PortaBilling_Ignore_Password:YES` RADIUS attribute in the authorization request.