PORTA ONE

PortaSwitch

New Features Guide

70
MAINTENANCE RELEASE

WWW.PORTAONE.COM

Copyright notice & disclaimers

PortaSwitch® New Features Guide, May 2018
Maintenance Release 70
V1.70.05

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 70 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.

GDPR compliance

GDPR (General Data Protection Regulation) is the EU regulation concerning personal data protection for EU residents. GDPR also regulates the transfer of personal data for processing by third parties outside the EU.

Personal data is information by which a person can be identified. Personal data includes name, address, phone number, MAC address of an IP phone, etc. Find the full list of personal data (defined by the administrator or provided by customers themselves) that may be stored in PortaBilling® in **Appendix A**.

To help you comply with this regulation the following enhancements are introduced in PortaBilling®:

- Anonymizing personal data on the PortaBilling® web interface and in API responses;
- Two-version PDF invoices: one that contains full information and another that contains only anonymized personal data;
- Adjusted email / SMS notifications received by administrators to anonymize personal data; and
- Recording user access to personal data in logs for troubleshooting and auditing purposes.

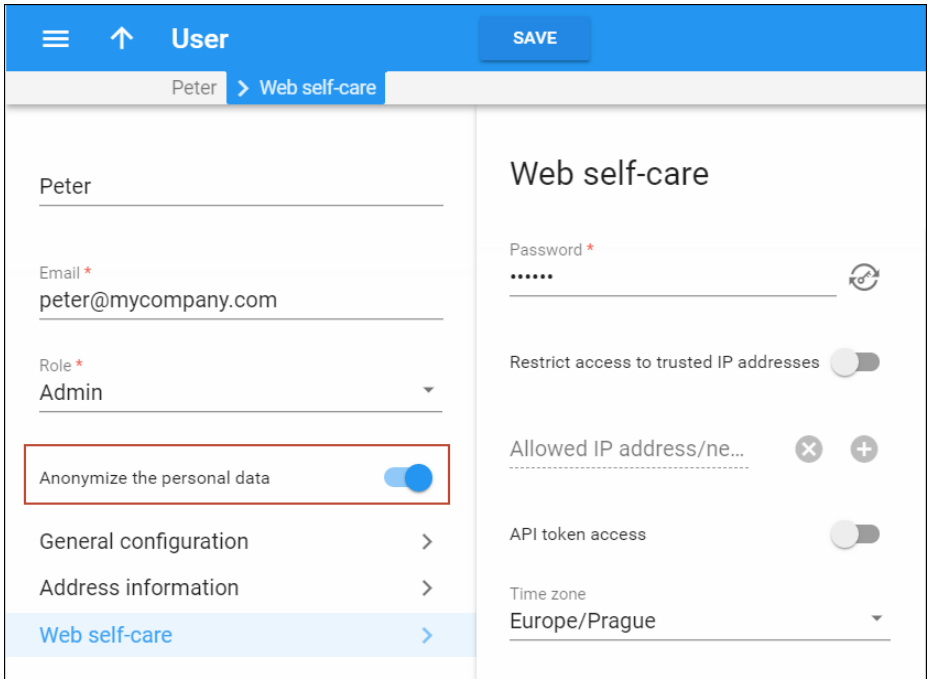
Personal data anonymization and access control

Now you can divide your administrative staff members into those who can see full customer details and those who are not allowed to process personal data.

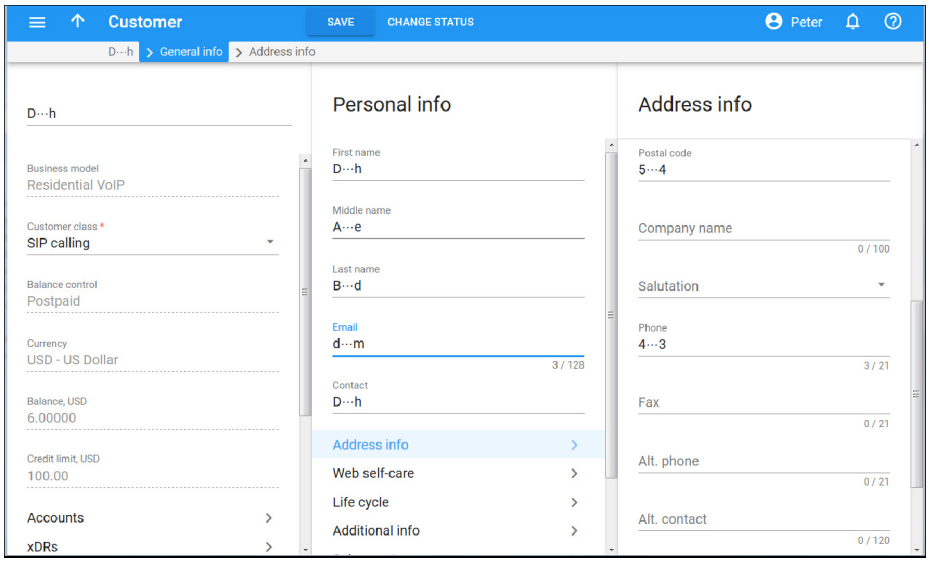
Consider the following example:
Let's say you provide services in France and your staff is in Paris, plus you have a remote administrator, Peter, in Montreal.

Peter must not process personal data without user consent and must not have access to it. Since you find it difficult to meet the GDPR requirements regarding personal data transfer and processing outside the EU, you decide to restrict Peter's access to personal data.

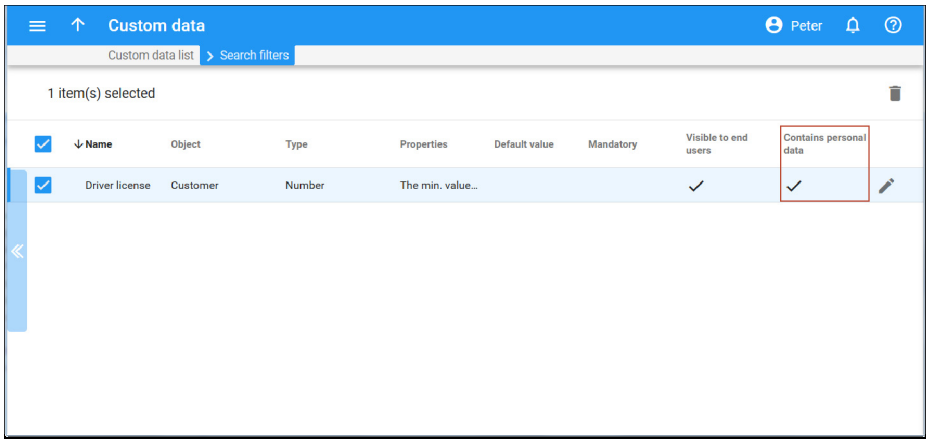
To do this, you enable the **Anonymize the personal data** option for his user in PortaBilling®.



This way, when Peter opens a customer's page, he sees that personal data is anonymized. When Peter receives an email or SMS notification that an invoice for a customer is re-generated, the customer name in the notification is also anonymized.



If you store additional information about your customers in custom fields and it could be considered personal (e.g. driver's license or insurance ID), you need to anonymize it, too. To make this happen, mark this field as containing personal data in PortaBilling®.



Though Peter can browse and modify customer details (e.g. assign add-ons to a customer account), he cannot change a customer's personal data nor access their self-care portal.

For the current MR70-0, Peter's activity in PortaBilling® has the following limitations:

1. Customer and account creation is forbidden.
2. Attachments such as account generation reports, invoices in invoice notifications, files with DIDs etc. are not available.
3. Access to SIP and BE logs is forbidden since the logs contain personal data. (Personal data anonymization will be added in future releases to grant access to logs.)
4. Previously generated custom reports are not available for download. Reports yet to be generated are available since the personal data in them is anonymized.
5. Additional information in xDRs (e.g. the actual phone number of a person making a call in an IP Centrex environment) is not available.
6. Access to a customer's old web interface is forbidden so that access to unanonymized personal data is prevented.

Beginning with MR71-0, MR70-1 will be enhanced to extend an administrator's access and operations. Please refer to the **Future enhancements** section for details.

The same logic applies when your staff manages personal data in PortaBilling® via the API from an external self-care portal.

By default, all personal data is anonymized using the same pattern – only the first and last symbols are shown. In future releases we plan to introduce the capability to customize personal data masking.

Two-version PDF invoice files

To protect personal data, PortaBilling® produces two versions of customer invoices:

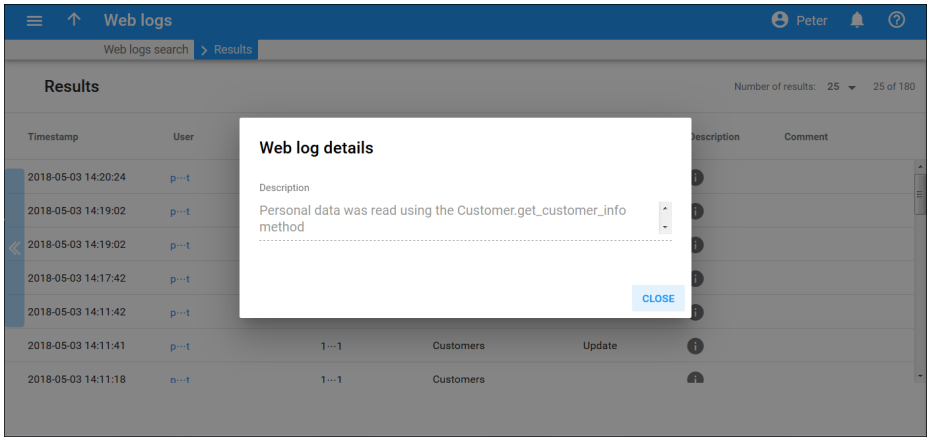
- Invoices with full data are generated for customers' use;
- Invoices with anonymized personal data are available for administrators who have restricted access to personal data.

Previously generated invoices are not available for download for these administrators either; however, they can adjust and re-generate such invoices, if necessary.

Logging user access to personal information

GDPR establishes requirements to record access to personal data by any user and consequently, to notify a supervisory authority should a personal data breach occur. Thus, service providers must track who processed personal data and when, and they must be able to prove it.

To meet these requirements, PortaBilling® records every user action that deals with personal information. So whenever an administrator with full access to personal data modifies a customer, the action is recorded in a log. Similarly, when a helpdesk operator with restricted access opens a customer panel, PortaBilling® logs the event.



This provides the ability to demonstrate the proper handling of personal data from creation to deletion. You can also provide proof of who exactly accessed personal data and a time stamp.

Future enhancements

Several enhancements are planned for PortaBilling® beginning with MR71-0, 70-1:

- The "right to be forgotten" functionality to respect users' rights to control their personal data. This provides for personal data to be cleaned up on demand.
- Personal data access control for your support staff provides you with the ability to create more flexible roles. Therefore, a full access role allows for the addition and /or modification of

personal data while a limited access role only grants access for viewing the data.
- Data anonymization in SIP / BE logs and in additional xDR fields to extend administrators' operations who have restricted access to personal data in PortaBilling®.
- Ability to control access to personal data for reseller CC staff members.

Integration with YateHSS/HLR

PortaBilling® is now integrated with YateHSS/HLR, which functions as a centralized subscriber database that stores and manages subscriber information for LTE service provisioning.

Wireless operators can provision subscriber data such as subscriber's phone number (MSISDN), SIM card IMSI and profile details (e.g. quality of service information) using PortaBilling® to activate SIM cards in HSS. Upon provisioning, a subscriber can then access the LTE service.

To provision subscriber data to YateHSS/HLR, an administrator creates a product for the LTE service and enables the **Mobile Network Provisioning** service for it. When a new mobile account is created, PortaBilling® sends the subscriber data to YateHSS/HLR via the External System Provisioning Framework (ESPF). With each change made to an account (e.g. an account is blocked or a new product is assigned), PortaBilling® synchronizes the information in YateHSS/HLR.

PortaBilling® is already integrated with YateUCN – another EPC component for real-time user charging. This integration with YateHSS allows wireless operators to use various Yate products to build and organize their network infrastructure.

Integration with Aricent HSS

PortaBilling® is now integrated with the Aricent HSS – LTE core network element that contains all subscriber data, such as:
- the account identification (the phone number (MSISDN) and SIM card, identified by IMSI), and
- profile information (e.g. static IP address, quality of service information).

This integration enables wireless operators to provision subscriber information defined within PortaBilling® to Aricent HSS, where a SIM card is activated by Aricent HSS and the LTE service becomes available for the subscriber.

To make this happen, an administrator enables the **Mobile Network Provisioning** service for a product and assigns it to an account with an associated SIM card. PortaBilling® then provisions the new subscriber information to Aricent HSS via the External System Provisioning Framework (ESPF). When an administrator makes changes for an account (e.g. blocking, changing a product), PortaBilling® automatically synchronizes this data with Aricent HSS.

This feature extends the list of LTE equipment that wireless operators can use for organizing their network infrastructure. For those operators that want to switch from legacy billing systems to PortaBilling®, the integration with Aricent HSS ensures the seamless migration of subscriber information.

Web cluster redesign

With this release, the web cluster setup has undergone the following changes:

1. **Usage of HAProxy as the load balancer within the cluster.** The previous approach to web cluster configuration required the virtual IP address to be up on all servers belonging to a web cluster. That required a special network configuration (to assign a multicast MAC address to each cluster node and configure the router to send incoming requests to all the servers using the unicast method) that some network equipment did not support.

   To simplify the web cluster configuration in terms of network, now the HAProxy load balancer is used. It accepts all incoming requests from users and applications and distributes them among web instances according to a predefined algorithm. The default algorithm is the "round robin," according to which requests are sent to each of the instances in turn.

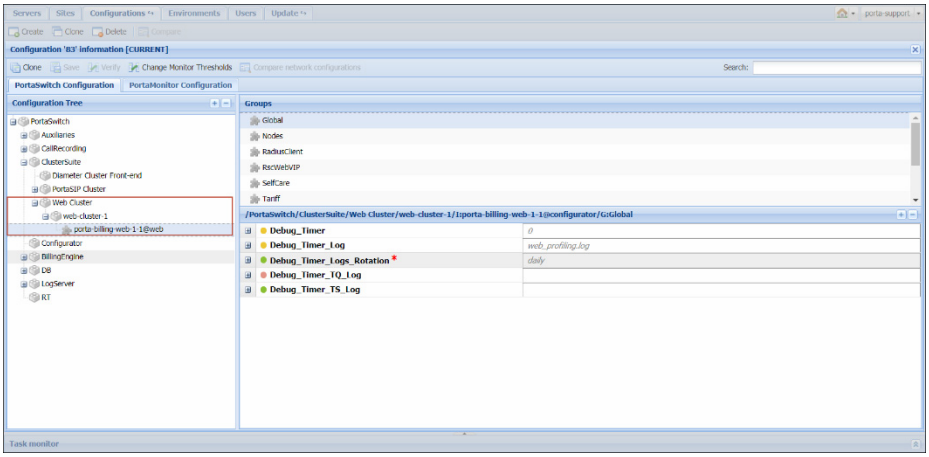
   The load balancer also monitors the state of web instances within the cluster. Whenever an instance is unavailable, it adjusts the request distribution. The HAProxy load balancing service is deployed on every web instance; however, it is only active on the instance which currently has the virtual IP address.

   This new approach simplifies the network configuration for a web cluster.

   If your installation has only one web instance, the load balancing service is not used.

2. **Simplified web cluster configuration.** Previously, to configure a web cluster, your administrator had to create both a porta-billing-web instance and a porta-cluster-web instance on every web server. Now they can create a single web cluster and then create web instances under it. Assign the virtual IP address to serve as the entry point to the cluster.

   Similar to a PortaSIP® cluster, a virtual IP address is shared among all web instances within the cluster but is only active on one of them. If the instance with the virtual IP address is down, it is enabled on another instance to ensure that services run without interruptions.



   If you do not use a web cluster in your system, create a single web instance under the web-cluster unit. In this case, the virtual IP address is not required, as access to web resources is done via the instance service IP.

   All web services' configuration parameters move to the WebCluster node on the Configuration server. Thus, all web clusters inherit the configuration defined at this level.

   This approach unifies the PortaSwitch® cluster configuration, making it transparent for the administrator.

Starting from MR70-0, both individual web instances and existing web clusters will be automatically reorganized using new architecture. If you utilize several individual web instances in your system, they will be placed under individual web clusters during the system update.

The web cluster redesign provides the following benefits:

- Simplified deployment and maintenance; and
- Auto-reconfiguration in case of an instance failure.

Enhanced API operation in dual-version PortaSwitch®

The API dispatcher in dual-version PortaSwitch® provides a single place for customer management and system operation while making the migration process more fluid. It accepts API requests from CRM applications, custom self-care portals, etc., and sends them for processing to the system where the customer record is located.

With this release, the API dispatcher has been enhanced to simplify operation for administrators and resellers as follows:

Session context auto-detection for API requests with mandatory customer / account ID.

Now the API application can send the request to update a customer in the alter-ego system without switching the session context from the main system. When the application sends the customer ID in the API request, the API dispatcher detects that this customer is located in the alter-ego system and runs the request there. After the customer is updated, the session context remains set to the main system, which enables the administrator to continue working there.

This enhancement reduces the number of API requests the application must send for customer management. As a result, this speeds up data processing and simplifies the interoperation of your API applications with PortaBilling®.

Note that the session context is auto-detected only for the API requests for customer and account management with mandatory `i_customer / i_account` in input parameters.

Preserving unique IDs for products, customer classes and service entities in dual-version PortaSwitch®

Some API applications use both unique IDs for customers / accounts and IDs of entities such as products, volume discount plans, etc. as static values in API requests. For example, to obtain information about a customer's volume discount plan usage, the application sends `i_customer` and `i_vd_plan` values in input parameters.

To preserve the workflow for these applications in dual-version PortaSwitch®, the IDs of products, volume discount plans and other service entities are preserved when moved between systems. Thus, when you migrate the ABC product with ID 123 to the alter-ego system, it remains 123. As a result, fewer customizations are required to make the API application compatible with dual-version PortaSwitch®.

The entities for which unique IDs are preserved are the following:

- Customers;
- Accounts;
- Customer classes;
- Destination groups;
- DID pricing batches;
- Number porting requests;
- Products; and
- Volume discount plans.

Differently from customers and accounts, these entities remain available in the main system even when moved to the alter-ego one. Therefore, the administrator must remember to modify them in both systems in order to avoid differences in configuration. For example, to modify a product, the application must:

- set the session context to the alter-ego system by sending the unique ID of this system's billing environment or the customer ID in the API request,
- send the API request to update the product configuration,
- switch the session context to the main system, and
- send the API request to update the product configuration in that system.

These enhancements simplify customer management in dual-version PortaSwitch® thereby making it more transparent for the administrator. They also reduce the workload required to make API applications compatible with dual-version PortaSwitch®.

Emergency call handling redesign

The idea behind emergency services is to provide users with a single short emergency number to dial (e.g. 112), that delivers their call to the relevant emergency service agency (police or ambulance, etc.). Since there can be several emergency service agencies within a country or city, it's crucial that the call is quickly routed to the emergency service center closest to the caller's physical location.

An emergency service center operator has access to a countrywide central emergency database that contains user phone numbers and addresses. When a call comes in to this service center, the caller's address is automatically displayed to the operator and they can quickly direct the emergency team to the caller.

As the service provider, you must ensure that the information about user locations is correct and regularly update the central emergency database with any changes.

A special emergency module in PortaBilling® handles emergency calls. PortaBilling® recognizes emergency calls based on the number dialed, searches for the corresponding record in the database to detect the emergency center number associated with the user and redirects the call to that number.

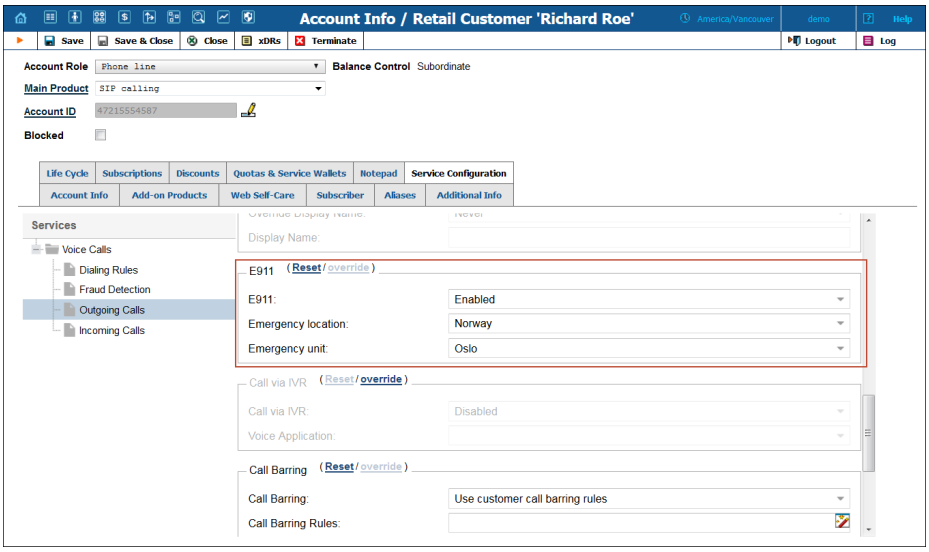
With this release, the emergency module has been redesigned and includes the following enhancements:

- **User location management via the API**. To enable a user's emergency services, an administrator must first associate an emergency service center number with the user location and then enter this information in PortaBilling®. The administrator now adds the user's location in PortaBilling® via the API. To speed up this process, an administrator can upload a user's location from a CSV file. This simplifies the data management for the administrator. In future releases, an administrator will be able to enter user locations from the web interface.

- **Routing by emergency administrative units.** Now PortaBilling® uses an "emergency administrative unit" mapping key that identifies the number for the appropriate emergency service center and redirects the call there.

  An emergency administrative unit defines user locations as a combination of their country and region pattern (e.g. a city or a ZIP code, etc.), separated by a dot. For example, if you provide services in Norway and identify an emergency call by the city and ZIP code it came from, the emergency administrative unit will be in the following format: no.Oslo.0131.

  Emergency administrative units are associated with the number of their corresponding emergency service center and stored in the PortaBilling® database. There can be several emergency numbers in a country (e.g. 110 for fire prevention, 112 for police and 113 for ambulance). To correctly redirect calls using the number dialed, you can define the routing rules so that calls to 110 are sent, for example, to 23255571 while calls to 112 are sent to 24155512.



After an administrator has added emergency administrative units to PortaBilling®, one is identified for a particular user's account. This way when a user dials an emergency number, PortaBilling® maps their emergency administrative unit with the corresponding record in the database, identifies the emergency service center number and instructs PortaSIP® to route the call there. Consequently, data mapping does not depend on user input. The use of a dot separator for emergency administrative units enables the proper handling of compound names (e.g. Kujawsko-pomorskie województwo in Poland).

If a user changes location (e.g. moves to another city), they must report it so that their location is updated in PortaBilling® and also forwarded to the central emergency database.

Thus, service configuration and user location management are simplified as a result of the redesigned emergency call handling feature. This ensures the proper provisioning of emergency call services and also meets legal compliance with the regulations in your country.

Universal ESPF provisioning handler

PortaBilling® introduces a new approach for provisioning data and executing interoperation with external systems. The External System Provisioning Framework (ESPF) now has a new EventSender provisioning handler, which is a universal handler that sends information about provisioning events to your external system where they are processed. This information is sent in JSON format via the HTTP protocol; thus, it can be read by any application. This allows you to

develop an integration plug-in for your external system in the programming language of your choice.

This is how it works:
Let's say you have several billing platforms and use a finance system which tracks income from all of them. You need to integrate this finance system with PortaBilling® to receive information about account creation / termination and payments made.

Since your development staff work in Java, they implement an application that receives HTTP requests with provisioning events and provisions them to the finance system in this programming language. Your administrator enables the EventSender ESPF handler in PortaBilling®, subscribes it to required events and then defines the URL of the application for it. Therefore, whenever a new payment is recorded in PortaBilling®, the EventSender sends this information to your finance system for processing.

The EventSender handler can subscribe to all supported events and operates in asynchronous mode by default. To prevent system overload in case of large numbers of events, the EventSender controls the number of parallel requests. And if necessary, you can always change the handler to operate in synchronous mode.

To provide an additional layer of security to communications between your external system and PortaBilling®, you can use a cryptographic signature for HTTP requests.

In summary, the EventSender handler has the following features:

- Sends events in JSON format;
- Can be subscribed to all supported events;
- Communicates with external system applications via the HTTP protocol;
- Operates both synchronously and asynchronously; and
- Supports the use of a cryptographic signature for requests.

This new approach to data provisioning simplifies integrating your external system with PortaBilling®. The ability for developing integration plug-ins in any programming language reduces implementation time and costs (e.g. enables you to engage your own development staff).

Auto-provisioning for new Grandstream IP phones

The list of IP phones that are auto-provisioned by PortaSwitch® has been extended to include the following phones:

- Grandstream GXP2135 (1.0.9.69 firmware version)
- Grandstream GXP2170 (1.0.9.69 firmware version)
- Grandstream GXP1760 (1.0.1.64 firmware version)
- Grandstream GXP1780 (1.0.1.64 firmware version)
- Grandstream GXP1782 (1.0.1.64 firmware version)
- Grandstream GXP1610 (1.0.4.106 firmware version)
- Grandstream GXP1615 (1.0.4.106 firmware version)
- Grandstream GXP1620 (1.0.4.106 firmware version)
- Grandstream GXP1625 (1.0.4.106 firmware version)
- Grandstream GXP1628 (1.0.4.106 firmware version)
- Grandstream GXP1630 (1.0.4.106 firmware version)
- Grandstream DP750 DECT base station with DP720 handsets (1.0.3.37 firmware version)

Click the link to find more information about any of the **Grandstream** IP phones.

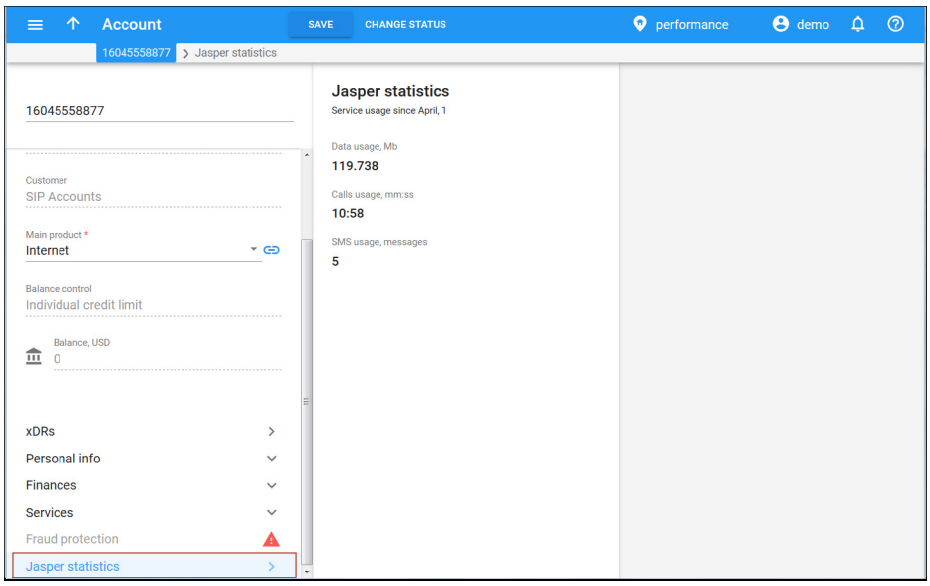
Auto-provisioning of these IP phones extends the number of offers you can make to your customers.

Other features and enhancements

- **Display service usage statistics from Cisco Jasper in PortaBilling®** – PortaBilling® is integrated with Cisco Jasper – the automated connectivity management platform. PortaBilling® provisions SIM card information to Cisco Jasper, enabling you to manage connectivity for subscribers. Cisco Jasper keeps track of their service usage and notifies PortaBilling® when a subscriber exceeds their allocated quota.

  Instead of browsing through subscriber details in both systems, you can now obtain full information about them on the PortaBilling® web interface. The integration plug-in available with this release enables you to display service usage details from Cisco Jasper in PortaBilling®.

After you have installed the plugin in PortaBilling®, the Jasper statistics panel appears for an account on the PortaBilling® web interface.



The panel contains information about the services used by a user within the current month: the total amount of data transferred, voice calls made and SMSs sent. If the user has exceeded the allocated quota, the administrator sees the corresponding notification in PortaBilling®.

Usage details are displayed for the current month and are updated on demand – when you open the page, the data is retrieved from Jasper.

Please contact the PortaOne® support team for assistance with how to install the integration plugin.

With this enhancement, you can perform account and service management from a single location.

- **Call records migration via Porter** – Now you can migrate customer call records between systems using the Porter data transfer tool. Consequently, customers can access and download them regardless of their current location in dual-version PortaSwitch®.

  As a rule, call recording service is configured on a separate server. Therefore, to migrate the call records, these following configuration steps are required:

- In the alter-ego system, provide access to your call recording server from the outside network for the data transfer. If the call recording server is deployed in a private subnet, assign a public IP address to it. Once the call records migration is complete, you can return the server to the private subnet.
- During data migration, call records will be added to a `/call-recording/wav` folder on the call recording server in the alter-ego system. Therefore, your user must have the write permissions for this folder to perform a data transfer.
- While migrating call records, Porter accesses the call recording servers on both systems via ssh. Therefore, make sure to provide ssh access to these servers for your user to perform the data transfer.

Since call record files can be large, run Porter to migrate the customer's main data. Afterwards, migrate the call records on the second run of Porter.

Please contact the PortaOne support team for assistance in making preparations and performing customer data migration.

This enhancement facilitates customer migration and ensures service integrity for your customers.

- **Custom report migration via Porter** – Custom report functionality enables administrators, resellers and representatives to obtain statistics information from PortaBilling® (e.g. cost / revenue statistics or charges per destination, etc.).

  With this release, the administrator can migrate custom report configurations between systems in dual-version PortaSwitch® by using the Porter data transfer tool.

  Porter transfers the following custom report data:
  - Custom report query – the input parameter (e.g. a customer) and output format values (e.g. number of visible columns) defined by the administrator for a particular custom report.
  - Custom report queue – the schedule according to which a custom report is executed. Porter migrates periodic and single time schedules that are defined for some moment in the future.

  The .csv files with report results are not migrated.

For a custom report to be successfully executed in the alter-ego system, the entity it is configured for (customer, vendor, reseller, etc.) must already exist there. Therefore, migrate the custom reports with the second run of Porter, once all required entities have been migrated.

For example, before migrating a commission report for your representative Anna Dow, make sure you already migrated customers to the alter-ego system that Anna Dow brought in and that her record also exists in the alter-ego system.

This enhancement ensures accurate reporting in dual-version PortaSwitch® and less configuration effort is required.

- **New PAI and IP authorization method** – The **PAI and IP** has been added to the list of suggested authorization methods for call handling. This authorization method allows service providers to charge external customers for the use of their services.

  For example, let's say that your reseller ABC owns an external system (e.g. a telephone system, a value-added platform, etc.). ABC would like to pass calls from their customers through PortaSwitch®. You consider the reseller's gateway as trusted and therefore trust data received from it.

  The gateway sends an authorization identity in the PAI header. PortaSIP® then uses the PAI value and IP address to authorize an account in PortaBilling®.

  The combination of **PAI and IP** ensures that PortaSwitch® only processes traffic from external customers who are registered on your system and then properly charges them.

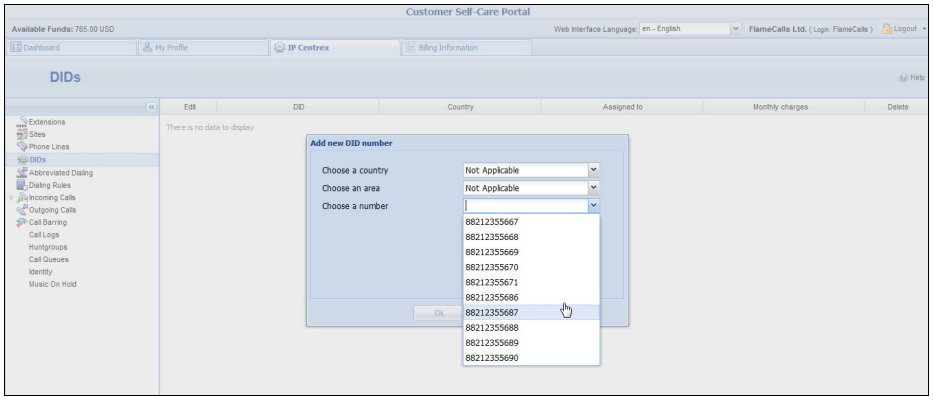
  You can also use this authorization method when the sending gateway does not support either digest authorization or tech prefixes.

- **Disconnect active sessions via API** – The list of API methods has now been extended with the **BillingSession.disconnect_session** method. With PortaSwitch®, telecom service providers can now disconnect voice calls and Internet sessions that are in progress.

  Be aware that your NAS must support session disconnect functionality in order to disconnect Internet sessions (i.e. RADIUS POD or DIAMETER DPR).

This enhancement gives telecom service providers an extra tool for coping with stalled sessions and / or potential fraud.

- **Customers provision DID numbers without country and area** – Some DID numbers have no geographical reference (e.g. start with a 882 code) and are uploaded to PortaBilling® without country and area. With this release, customers can provision these non-geographically identified numbers via their self-care interfaces. These DID numbers appear on the list when customers select **Not Applicable** for country and area fields.



This enhancement broadens the range of DID numbers that customers can provision for themselves.

- **Prorating of volume discount plans** – Prorated volume discount plans permit a quota to be recalculated depending on the number of days left until the end of the current billing period. With this release, the proration schema has been changed so that if a volume discount plan is changed / assigned *before* 10:59 p.m., the day of change / assignment is included in the proration for the newly assigned plan. Let's consider when a volume discount plan is:
  - changed in the middle of a billing period; or
  - assigned on the last day of a billing period.

Volume discount plan change in the middle of a billing period

Consider these examples when counters for the previous volume discount plan are preserved for use with the new one.

- Mary Smith is granted 60 minutes of free calls. By November 15th she wants to upgrade to a new quota of 100 minutes. She switches over to the new product and since she made 20 minutes' worth of calls during 14 days, there are still 8 minutes (60*14/30-20=8) available from the previous quota. The newly assigned quota is prorated for the 16 days left till the end of the month

(100*16/30=53). With the unused minutes from the previous quota added, Mary receives a total of 61 minutes (8+53=61) of free calls for November.

- Mark Johnson does something similar. He made 59 minutes' worth of calls (almost the whole quota) during 14 days, so 31 minutes (60*14/30-59=-31) would be deducted from the new prorated quota (100*16/30=53). Thus Mark only has 22 minutes available (-31+53=22) till the end of November.

When counters are not preserved, a user receives the prorated quota only from the newly assigned volume discount plan.

- Let's say Richard Roe also switches over to a new product on November 15th that has a quota of 100 minutes. He made 59 minutes' worth of calls during 14 days. This quota is not prorated since the counters are not preserved so Richard receives 53 minutes (100*16/30=53) of free calls for November.

Volume discount plan assignment on the last day of a billing period

If a volume discount plan is assigned on the last day of a current billing period:

- *before* 10:59 p.m. – services are available during the entire day. The quota is prorated, bringing the available amount of services for the whole day;
- *after* 11:00 p.m. – services are unavailable till midnight. The quota is prorated when the following billing period begins.

For instance, John Doe has a monthly billing period. At 6 p.m. on April 30th (the last day of his billing period) he assigns an add-on product that contains a quota of 100 minutes of free international calls. As a result, John receives 3 minutes of free calls (100*1/30=3), since the quota was prorated for the last day.

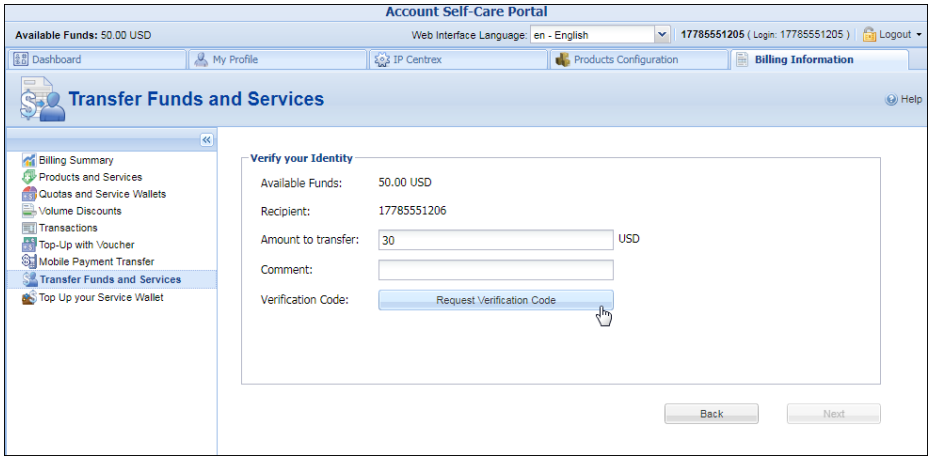
This enhancement makes the volume discount plan proration schema more user-friendly and meets user expectations.

- **Transfer funds for credit accounts with individual credit limits** – With the transfer of funds functionality, end users are able to transfer money from their balances, e.g. to pay for goods or top-up their relatives' balances.

  With this release, in addition to debit accounts, credit accounts with an individual credit limit can both transfer and receive money. To make this happen, an administrator enables the

Subscriber-to-subscriber transfers option either at the customer or customer class level. Note that only a prepaid amount of money can be transferred.

For instance, let's say user Richard Roe has prepaid $50. He visits his self-care interface and transfers $30 to his sister, Mary Smith, since she ran out of money. Mary receives $30 and Richard's prepaid amount is now $20.

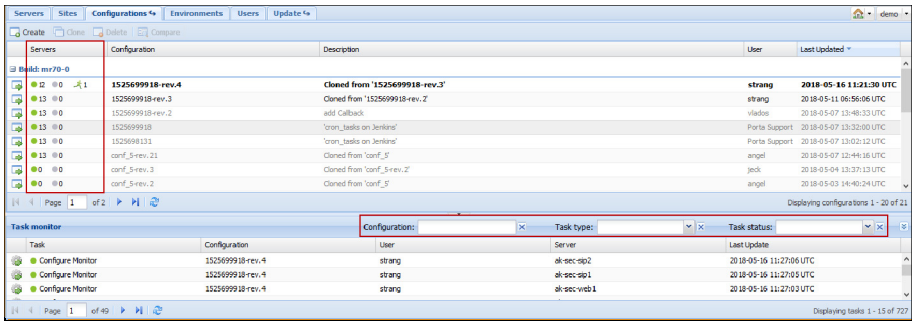


This enhancement enables service providers to increase their revenue by encouraging their end users to top up their balances regularly.

Web interface changes

- **Enhanced configurations display and troubleshooting** – With this release, an administrator sees the number of servers that a new configuration has been applied to or failed on. They can also filter configuration tasks to troubleshoot an issue quickly.

  The existing configurations are now marked as follows:
  - "**active**" (i.e. current) is **bold black**.
  - "backup" (i.e. previous) is black.
  - "inactive" (i.e. old / new) is grey



The **Servers** column has been added to the Configurations tab. It contains clickable indicators that show the state of applying the configuration:

- **green** (i.e. succeeded) indicates that a new configuration was applied successfully,
- **grey** (i.e. failed) indicates the absence of errors,
- **red** (i.e. failed) indicates that errors are detected,
- **a running man** (i.e. running) indicates that the configuration is now being applied,
- **a number** (e.g. 13) to the right of the indicator shows the number of servers involved.

  When you click a successful or failed indicator, those tasks are automatically displayed in the **Task monitor** window.

The search filters have been added to the **Task monitor** window:

- **Configuration** – filters the tasks based on the configuration name.
- **Task type** – filters the tasks based on the task type (e.g. Commit configuration).
- **Task status** – filters the tasks based on the task state (e.g. failed, running, etc.)

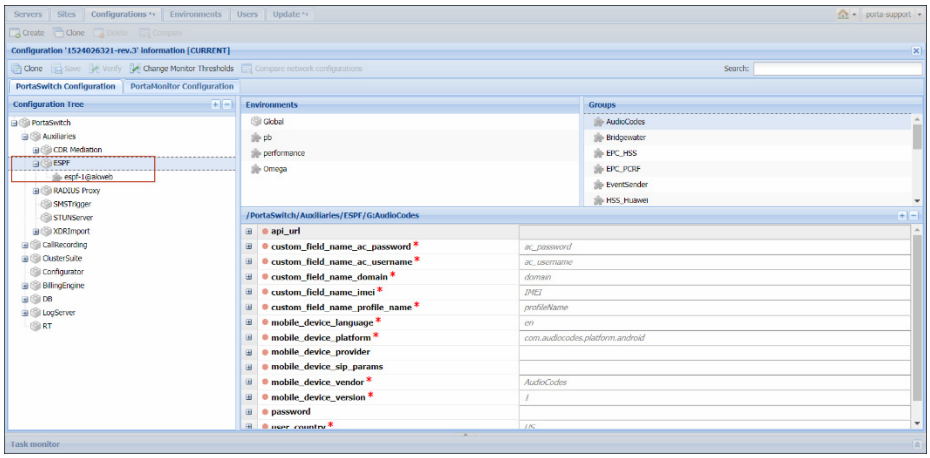
These enhancements simplify monitoring and troubleshooting for administrators and make the Configuration server web interface more user-friendly.

Important upgrade notes

- **The ESPF as an independent system component** – The External System Provisioning Framework (ESPF) serves to provision customer information and service configurations to external systems that are integrated with PortaBilling®. For example, as an MVNO, you need to provision SIM card information to the HSS to activate SIM cards for your subscribers.

Previously, the ESPF used the modules of the admin (web) server and could only be configured on that server. Now it is an independent system component and has the following features:

- It uses the PortaBilling® API to communicate with the database and retrieve data. This simplifies the support for custom handlers during system updates.
- It is represented as a dedicated ESPF node on the Configuration server.
- The ESPF instance can be configured on any server in the main site but only one instance per server is allowed.
- The ESPF can be scaled up by adding more instances.
- Configuration parameters for every external system that is integrated with PortaBilling® are now organized into corresponding groups under the ESPF node. This simplifies the configuration process for the administrator.



Both admin and ESPF components use the same configuration parameters (e.g. the URL for accessing the IPTV provider's API server) in IPTV and Number porting service provisioning. Therefore, both IPTV and Number porting configuration parameters have been moved under the PortaSwitch® node on the Configuration server for common use.

During a system update, the ESPF service will be automatically enabled on the web server if it was configured to do so beforehand. However, additional configuration parameters for an external system defined in the WebCustom option in previous releases must be manually enabled after a system update.

- **One execution schedule per custom report** – With this release, custom reports have a single execution schedule. This ensures their proper execution and prevents misconfiguration and / or errors in reporting.

Custom reports with several execution schedules are considered as separate reports. Therefore, such custom reports must be reconfigured to contain a single schedule before a system update. To make this happen:

- clone a report and assign one of the schedules to it;
- delete this schedule for the original report.

- **PrinceXML for PDF invoice generation from all template types** – To help you comply with GDPR requirements for personal data protection, PortaBilling® generates two versions of PDF invoice files: one version contains full personal data to be used by customers. The other version contains anonymous data to be used by members of your administrative staff who have restricted access to personal data.

  To support data anonymization on invoices, PortaBilling® now uses PrinceXML software to generate PDF files from templates created both externally and by using the default layout designer. This also removes the intermediary steps required by the previous Apache FOP generator and unifies the invoice generation process.

  Invoices from existing default templates may have slightly different margins, colors, frames, etc. when generated via PrinceXML. Therefore, verify the invoice layout by clicking the **Preview** icon next to the invoice template to be sure it is correct.

- **Support for TLSv1.2 only** – According to the latest PCI Data Security Standard, PortaBilling® only supports the TLSv1.2 now. Since modern browsers such as Google Chrome and Mozilla Firefox support higher versions of TSL protocols by default, your users are not affected.

  If you have any customized Apache web server configurations (i.e. you generated additional configuration files that are not managed via the Configuration server), change them so that they only contain secure TLSv1.2 protocols.

- **Emergency call routing by emergency administrative units** – With this release, PortaBilling® routes emergency calls to a local emergency service center based on an emergency administrative unit associated with an account. An emergency administrative unit defines a user location as the combination of their country and region pattern (e.g. no.Oslo.0131), and is associated with an emergency service center's number.

  To preserve your emergency service configuration during a system update, a special migration script is available in PortaBilling®. It

analyzes existing address key values for accounts in the database and forms emergency administrative units. Then it adds corresponding emergency administrative units within an account's service configuration.

The script employs two modes of operation:

- the "test" mode checks the emergency service configuration for accounts and returns records that cannot be updated automatically. This allows you to correct the configuration before a system update to ensure that the data is migrated correctly; and
- the "migration" mode which performs the data transformation.

Emergency administrative units are stored in a new Voice_Emergency_Routing_Units database table. For backward compatibility, the E911_Administrative_Units table is preserved but is now considered obsolete.

Appendix A. Personal data that can be stored in PortaBilling®

The table below lists the kinds of personal data that can be stored in PortaBilling® and defines the availability for users with restricted access to personal data.

Entity	Personal information	Anonymized	Not available
Customer and reseller	Name	Y	
	Billing address information	Y	
	Address information including country, state, city, ZIP code	Y	
	Contact information such as company name, email, phone numbers, fax, BCC email	Y	
	Credit card details	Y	
	Additional fields in xDRs		Y
	Custom fields	Y	

	Sales agents' names		
	Self-care credentials	Y	
	Invoices	Y	
	xDRs	Y	
Account	ID	Y	
	Service password	Y	
	Subscriber details such as name, email, phone numbers	Y	
	Address information	Y	
	Contact information	Y	
	Aliases	Y	
	Phone book details	Y	
	Follow-me lists	Y	
	Abbreviated dialing lists	Y	
	SIM card information: IMSI, MSISDN	Y	
	IP phone details: IP address and port, MAC address	Y	
	xDRs	Y	
	Additional fields in xDRs		Y
	Call records		Y
	Voicemails		Y
	Credit card details	Y	
	Self-care credentials	Y	
Vendor	Name	Y	
	Address information including country, state, city, ZIP code	Y	
	Contact information such as company name, email, phone numbers, fax, BCC email	Y	
	xDRs	Y	
	Self-care credentials	Y	
Representative	Name	Y	

	Address information including country, state, city, ZIP code	Y	
	Contact information such as email, phone numbers, fax, BCC email	Y	
	Initials	Y	
	Self-care credentials	Y	
CC_staff	Name	Y	
	Address information including country, state, city, ZIP code	Y	
	Contact information such as email, phone numbers, fax, BCC email	Y	
	Self-care credentials	Y	