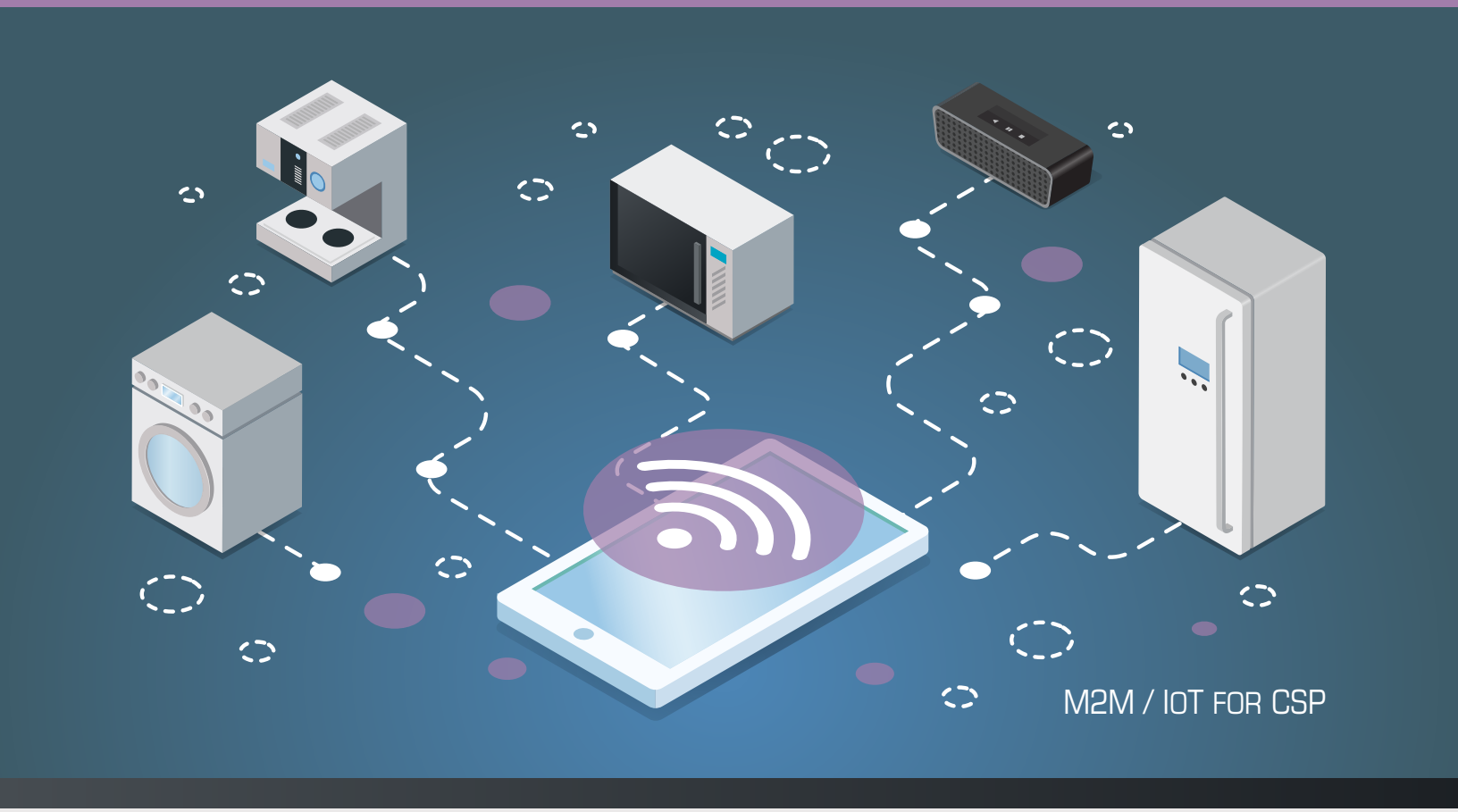
PORTA ONE




# PortaSwitch

## New Features Guide

74

MAINTENANCE RELEASE



WWW.PORTAONE.COM

# Copyright notice & disclaimers



**PortaSwitch® New Features Guide, November 2018**
**Maintenance release 74**
**V1.74.05**

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 74 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.

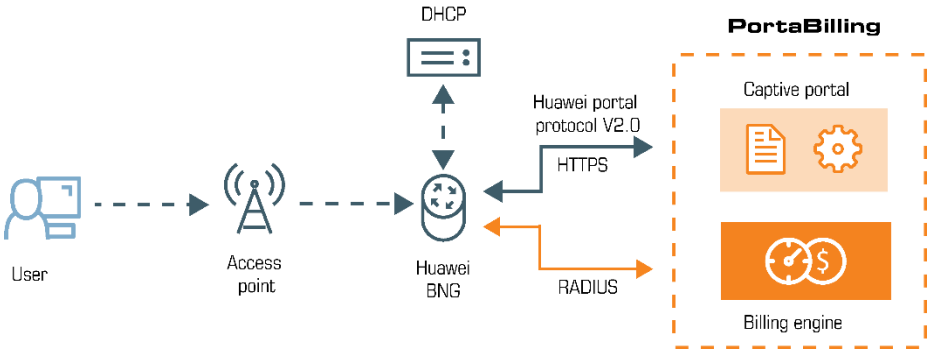
# Captive portal for WiFi hotspots

As of this release, PortaBilling® has a captive portal for WiFi hotspot services. This allows you to configure WiFi access points in various public places (e.g. cafes, gyms, hotels, etc.), enable users to easily subscribe and access WiFi using vouchers. To promote your service you can also configure PortaBilling® to grant one-time free minutes (e.g. 15 minutes of free WiFi access per day).

The supplied captive portal interoperates only with Huawei BNG (Broadband Network Gateway) and is a sample model. Your in-house or outsource developers can extend it to interoperate with the WiFi routers and access points that you use. Alternatively, they can use it as a basis when building your customized captive portal.

The captive portal is located on the PortaBilling® web server and consists of:

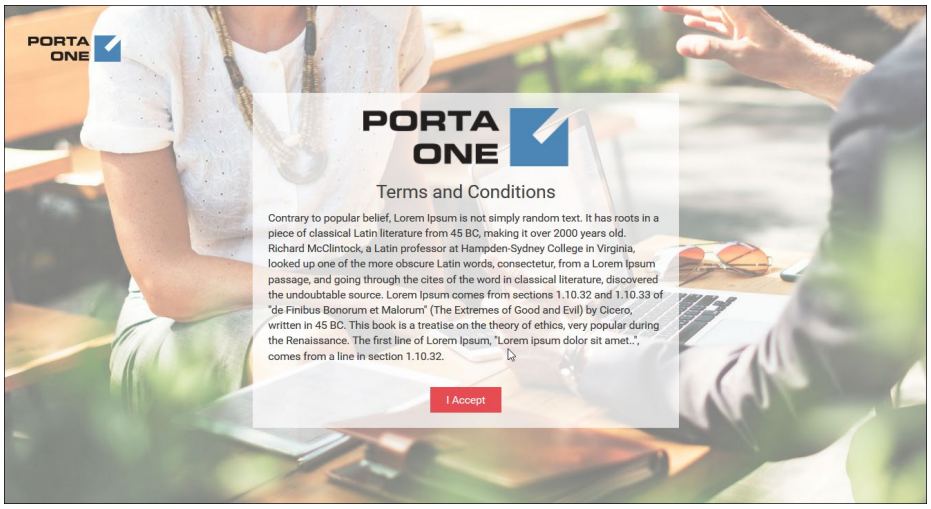
- A front-end web application – This is the set of webpages to which users are redirected when they open a web browser. These pages contain your legal information (name, logo and the terms of use), provide signup / login options and show available prepaid plans. They also return user credentials for subsequent logins upon signup, display the session status and the remaining time available. You can customize the content, page design and layout (e.g. use your pictures and colors) as you like.
- The back-end signup module. This communicates with PortaBilling® via the API to create user accounts. It also communicates with Huawei BNG via Huawei portal protocol V2.0 to pass the user credentials and their device IP address to PortaBilling® for authorization. Upon your request, other communication protocols can be added to integrate the signup module with another BNG or router you use.



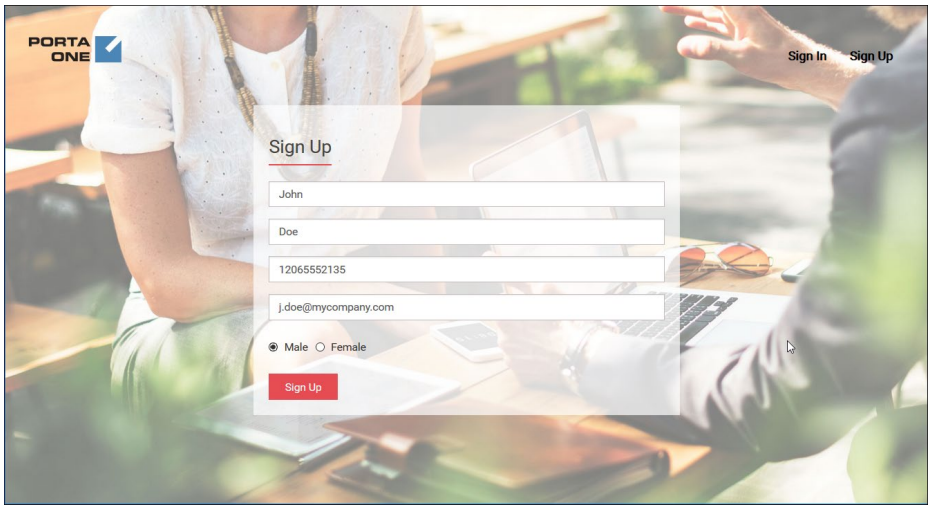
To illustrate how the captive portal works, consider the following example:
Let's say you provide the following WiFi access options:

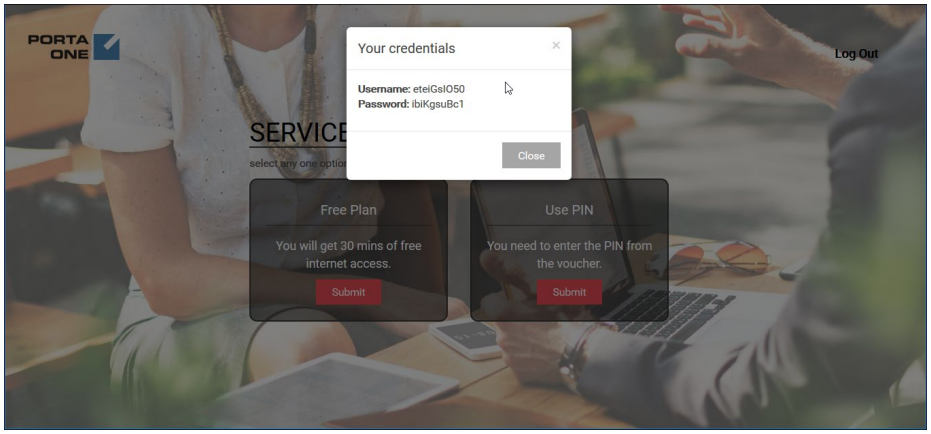
30 free minutes per day;
$10 vouchers for 1 hour; and
$15 vouchers for 2 hours.

John Doe wants to use the Internet, so he purchases a $10 voucher. When he connects to WiFi, his device is assigned an IP address by the DHCP server. He opens the web browser and the BNG redirects him to the captive portal to accept the terms of use.

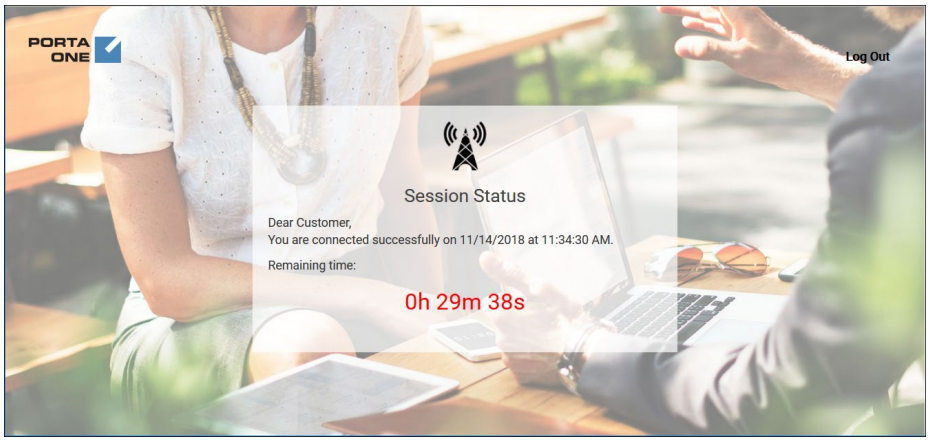



Then a sign up screen appears so he enters his name, email, gender and phone number. The signup module creates an account for him in PortaBilling® and the portal's webpage shows his credentials for further logins.






John can choose to use free minutes or enter the voucher PIN. He chooses the free minutes first. The signup module sends John's credentials and the device's IP address to the BNG. The BNG authorizes the account in PortaBilling®, receives the session duration time from PortaBilling® in the response and activates his Internet access.




When the free 30 minutes expire, the BNG sends the accounting information to PortaBilling® and redirects John to the captive portal. John must enter his voucher PIN now to use the Internet. When he enters it, PortaBilling® authorizes his account for one-hour access and the BNG resumes his session.

After 45 minutes, John closes the session. He still has 15 minutes of Internet usage available that he can use by logging in with the credentials provided.

Thus, with PortaBilling® and the captive portal you can generate revenue by selling WiFi vouchers and providing WiFi connectivity in public places like cafes, hotels, libraries, airports, etc.

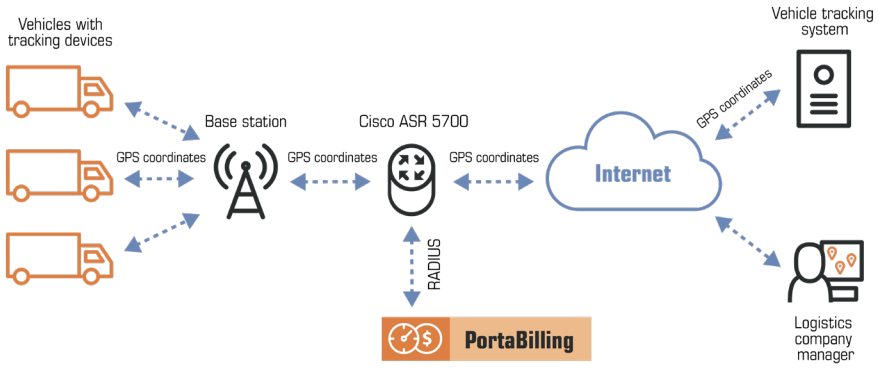
# Integration with Cisco ASR 5700

PortaBilling® is integrated with the Cisco ASR 5700. This is a GPRS Gateway Support Node (GGSN) that routes data traffic between a mobile network and an IP-based network (the Internet). This integration enables wireless operators to deliver M2M connectivity services, bill customers for their Internet usage and control session availability.

Cisco ASR 5700 performs the functions of a network access server (NAS). It communicates with the PortaBilling® OCS (Online Charging System) via the RADIUS protocol to authorize M2M devices and send accounting requests. PortaBilling® performs real-time charging for Internet access services.

Consider the following example:

A logistics company wants to track their vehicles. Each vehicle has a device with a SIM card to send GPS coordinates over the Internet. When a device establishes a data session, Cisco ASR 5700 sends an authorization request to PortaBilling® to verify that the account (which represents a device in PortaBilling®) has sufficient funds / quota and is permitted to use the service. It periodically sends interim (also called keep-alive) accounting requests with information about the volume of consumed traffic. Based on that information, PortaBilling® verifies whether a device can continue to send data. If there are no funds (or quota), Internet access is no longer available and the GPS coordinates cannot be sent.




**NOTE**: Cisco ASR 5700 does not support PoD (Packet of Disconnect) and CoA (Change of Authorization) requests. To avoid overdrafts, use an external application to check the account's (device) balance / quota and disconnect an Internet session.

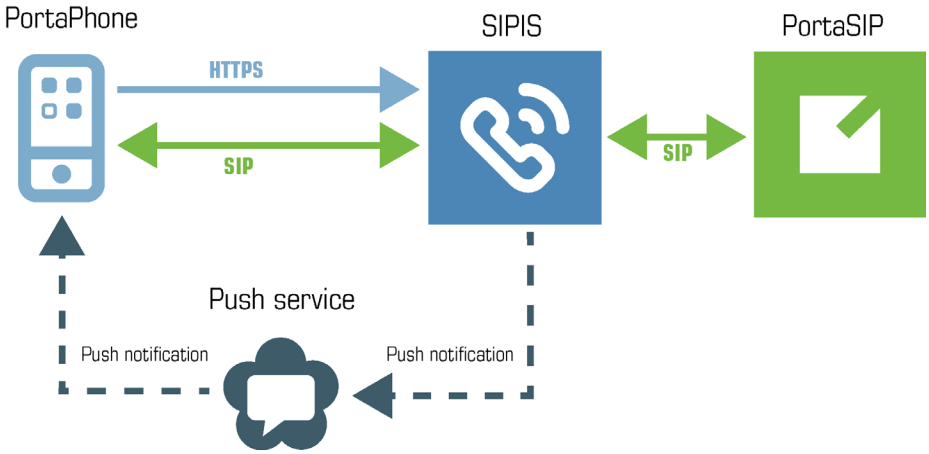
This integration enables wireless operators to extend the variety of equipment for providing M2M connectivity services.

# Hosting Acrobits Push server in PortaSwitch® for PortaPhone

Now you can deploy the Acrobits push server (SIPIS) in PortaSwitch® to send push notifications to PortaPhone users. Push notifications ensure that users receive incoming calls and / or messages while PortaPhone is either closed or in the background consuming little battery.

By deploying SIPIS in PortaSwitch®, your costs for push notifications do not depend on the number of users you have, as these costs are part of a PortaPhone SaaS subscription. In addition, user SIP credentials required by SIPIS stay within your PortaSwitch® installation.

SIPIS operates as an active proxy. It communicates with PortaPhone via the HTTPS protocol to obtain user SIP credentials for registration. It communicates with PortaSIP® via the SIP protocol to register on behalf of the phone user and handle incoming calls and messages when PortaPhone is in the background.

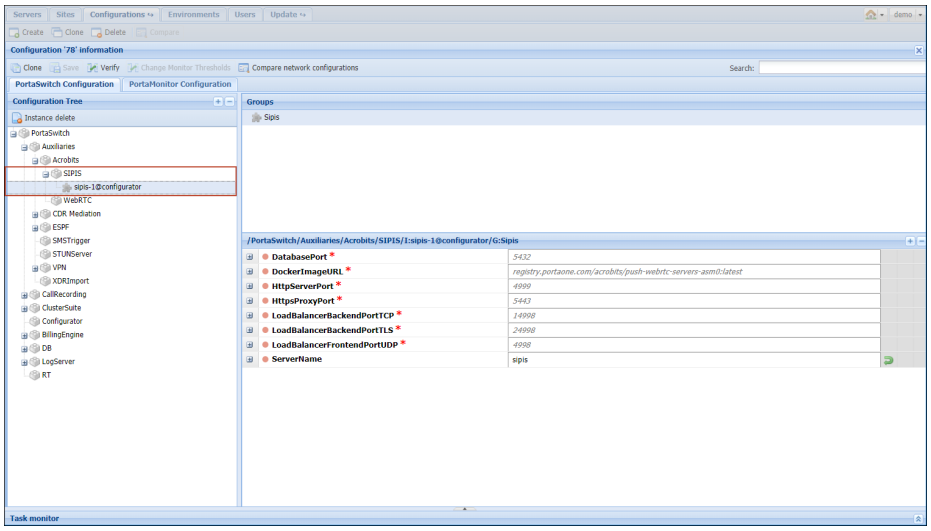



Let's have a closer look at how it works:
When PortaPhone is open and in the foreground, it is registered on PortaSIP® and thus receives all calls and messages directly. When it is moved to the background, PortaPhone unregisters on PortaSIP® and sends the HTTPS request with the user's SIP credentials to SIPIS. SIPIS then registers on PortaSIP® and begins to monitor for incoming calls and messages.

When there is an incoming call, PortaSIP® sends it to SIPIS. SIPIS sends the push notification to the user's phone via either an Android or iOS push service. This wakes up PortaPhone. Then SIPIS initiates the call with PortaPhone and once the call is established, it mediates the SIP signaling between the calling party and the user's phone. The RTP stream

flows directly between the phones. In such a way, the user receives the call as if the app had been running.

To configure SIPIS in PortaSwitch®, create the SIPIS instance on the Configuration server and define the server's hostname there. The system activates it automatically.



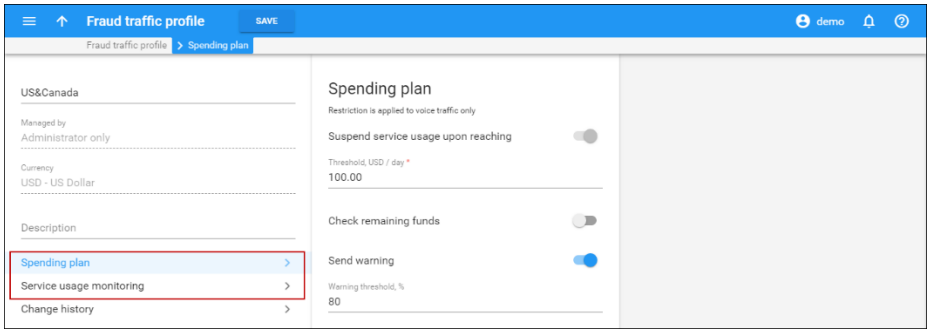

Push notification processing is a resource consuming task and highly dependent upon the number of anticipated users (e.g. to process up to 5000 users, 64 bit CPU, 4GB RAM and 30GB of disk space are required). Therefore, we recommend that you deploy SIPIS on a dedicated server. The SIPIS server requires a valid SSL certificate issued for the server's domain name and signed by a trusted Certificate Authority (e.g. LetsEncrypt). This ensures its normal operation with iOS devices.

# Unified tool for fraud traffic prevention

With PortaSwitch®, service providers can minimize their customers' / resellers' financial losses in case of fraudulent activity by using the following fraud prevention tools:

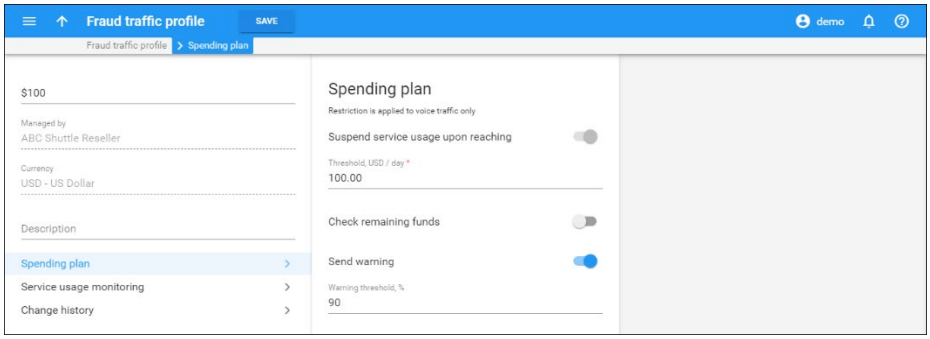
- **Spending plan**. This allows administrators to limit customers' / resellers' daily expenses on voice calls and receive alerts once a specific limit is reached,
- **Service usage monitoring** (previously known as a **Fraud traffic profile**). This allows administrators to set the expected volume of voice traffic to be sent by their customers to unusual destinations (e.g. Somalia or Albania, while VoIP services are mostly used for the USA and Canada) and receive alerts once a threshold is reached.

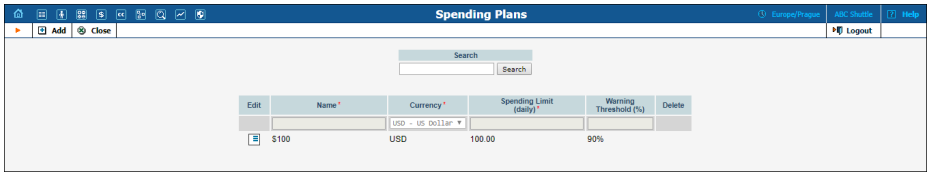
With this release, fraud traffic prevention tools have been united and are referred to as a **Fraud traffic profile**. An administrator can now configure a spending plan and service usage monitoring thresholds in a single place. This simplifies their configuration of fraud traffic prevention.




Fraud traffic profiles can be used by resellers to track their customers' daily expenses on voice calls and notify a reseller when a customer's spending threshold is reached.

Fraud traffic profiles can be configured only via the new web interface. Since the reseller self-care portal is still on the old web interface, resellers see their fraud traffic profiles as spending plans.




## Fraud traffic profile management via the API

Both administrators and resellers can manage fraud traffic profiles via the API. To make this happen, they must now adjust their API applications to use new API methods for the `TrafficProfile` service.

Previous API methods for managing spending plans (`SpendingPlan` service) and fraud traffic profiles (`FraudTrafficProfile` service) have been discontinued.

When updating to Maintenance Release 74, the system checks which fraud prevention tools were applied to the customers and resellers: spending plans, service usage monitoring profile or some combination thereof. Based on this data, the system creates new fraud traffic profiles for a customer / reseller that preserve the configuration of the spending plan and / or service usage monitoring profile.

# Remaining spending amount check for call authorization

A spending plan enables you to limit your customers' daily expenses on voice calls and minimize their financial losses in case of a hacker's attacks. PortaBilling® now calculates a customer's remaining spending amount during call authorization and re-authorization. If the remaining spending amount is lower than available funds / credit limit, PortaBilling® uses it to authorize calls. This increases fraud protection.

The following example illustrates how it works:

Let's say that your SIP trunking customer EasyCall is assigned a $100 spending plan. EasyCall has a credit limit of $1000 USD and a balance of $200 and they are allowed to establish 10 simultaneous calls. When authorizing each new call, PortaBilling®:

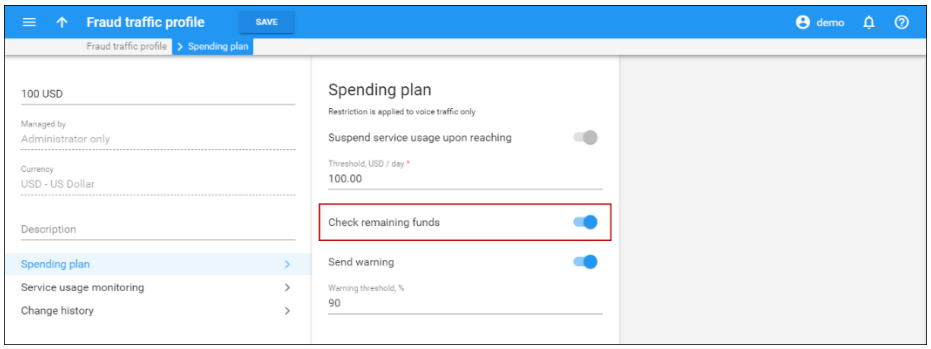
- checks the customer's available credit amount ($800) and compares it with the remaining spending amount ($100).
- since $100 is less than $800, PortaBilling® calculates the call duration based on the remaining spending amount ($100).

When any of the calls in progress are re-authorized, PortaBilling® checks the remaining spending amount and calculates the call duration based on that.

Every time a call ends, the remaining spending amount decreases. Accordingly, PortaBilling® reduces the maximum call duration when it authorizes and re-authorizes calls. Once the spending limit is reached, PortaBilling® rejects all following authorization / re-authorization requests. Calls in progress last only for their previously authorized time.

Note that PortaBilling® does not lock funds from the remaining spending amount when it authorizes calls. Therefore, customers may still exceed their spending limit if a call in progress lasts too long and have therefore high cost by the moment the spending limit exceeds. For example, if the customer has only $1 left out of the $100 spending limit and the call for $10 ends, their total amount spent becomes $109.

An administrator enables this feature for a spending plan, when a Fraud traffic profile is created.




### Spending plan and overdraft protection settings

The remainder of the spending amount can override the overdraft protection configuration if it is less than the amount to be locked for a call.

Let's say that an administrator has configured PortaBilling® to lock at least $10 per call and the customer is allowed to call A-Z destinations for a unified price of $1 /min. The customer's remaining spending amount is now $8.

When a customer makes a new call, PortaBilling® compares the amount to lock ($10) with the remaining spending amount ($8). Since $8 is less than $10, PortaBilling® reduces the amount to be allocated for the call by up to $8. PortaBilling® then calculates the maximum call duration based on $8. Thus, it authorizes the call to last eight minutes and therefore locks $8.

This enhancement allows you to adjust the maximum permitted duration of calls in accordance to customers' daily limits. If your gateway is incapable of dynamic re-authorization and your customers are allowed to establish multiple simultaneous calls, it minimizes their financial losses in the case of fraudulent activities.

# Other features and enhancements

- **VPN for PortaSwitch® sites deployed on the premises and in the cloud** – Now you can interconnect PortaSwitch® sites that are deployed both on the premises and in the cloud by using the built-in VPN solution. The VPN client in PortaSwitch® now supports VTI mode, in which encrypted network traffic is routed from one site to another through virtual tunnel interfaces (VTI)

that are enabled for VPN endpoints in a tunnel. This meets the Oracle Cloud Infrastructure recommendations used to deploy cloud-based PortaSwitch® for building IPSec VPN tunnels.

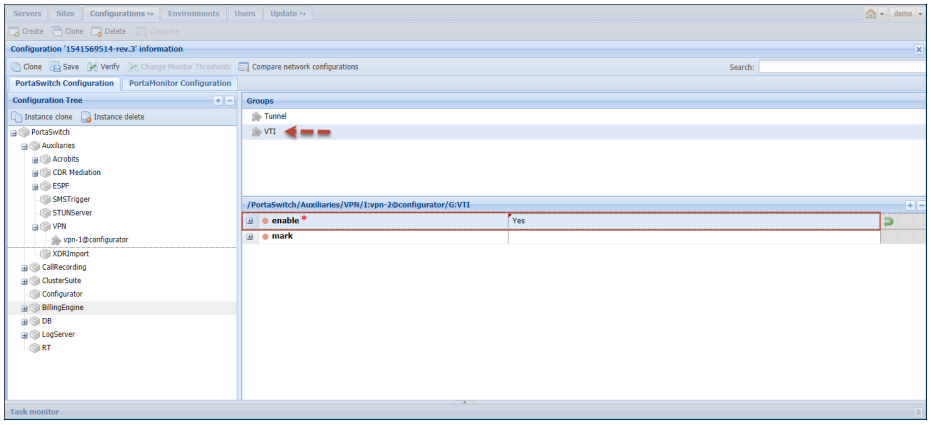
To interconnect PortaSwitch® sites via the VPN, the following must be done:

- set up a VPN endpoint for the cloud-based site;
- set up a VPN endpoint for the on-premises site;
- enable the VPN tunnel between the sites.

PortaOne support handles a VPN endpoint configuration for the cloud-based site. Once configured, you receive its public IPv4 address, the pre-shared key and a private cloud network address.

To set up a VPN endpoint for an on-premises site, create the VPN instance and enable the VTI mode for it on the Configuration server. Provision the information about your cloud-based VPN endpoint, the VPN endpoint's IP address and the IP address for the private on-premises network within the VPN instance configuration.

Note that VTI VPN tunnels are not supported for sites hidden behind NAT; thus, your on-premises VPN endpoint's IP address must be public.

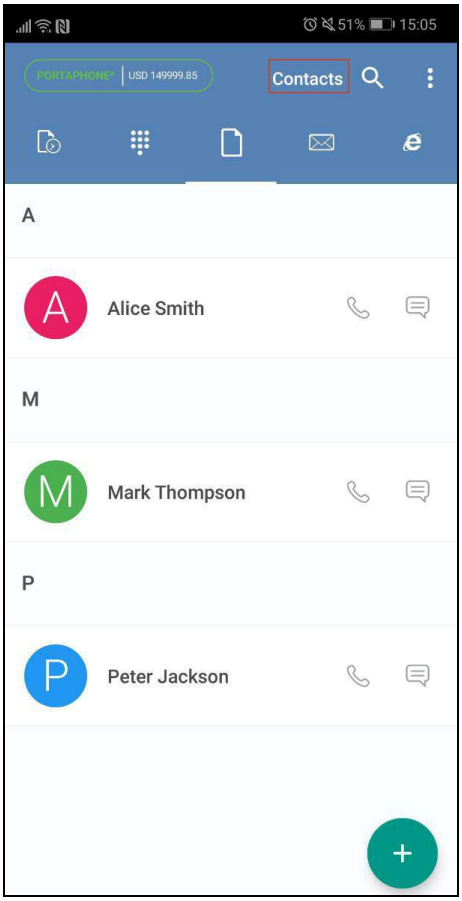



When the system applies the configuration, it establishes the VPN tunnel and routing between the cloud-based site and the on-premises site.

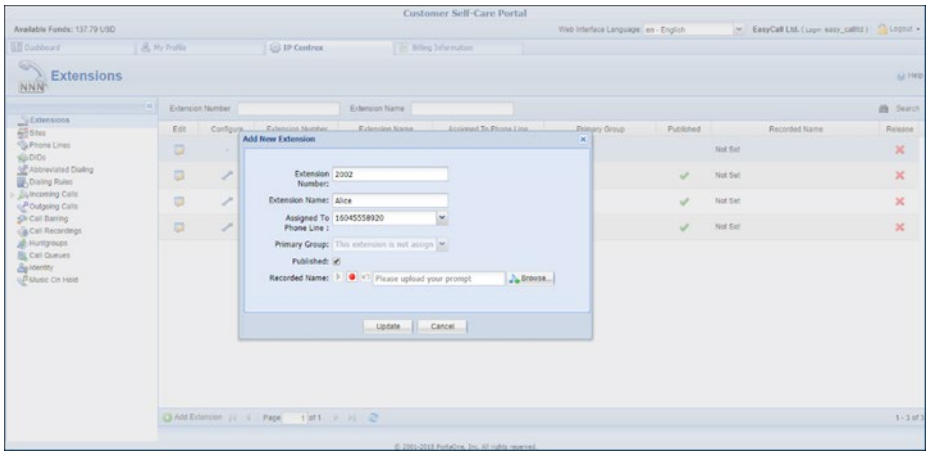
This enhancement enables your administrators to organize a VPN network by means of a PortaSwitch® VPN client so it unifies the network configuration for the entire system.

- **Display extensions list in PortaPhone** – Now IP Centrex PortaPhone users can see a list of their colleagues' extensions on

the **Contacts** tab. All they need to do is switch the contact source from the phone address book to **Contacts** in PortaPhone. Thus, users can quickly find a person by name so they don't need to remember everyone's extension number or search elsewhere for it.




Extensions management is done in PortaBilling® via the customer self-care. When a customer adds a new extension, PortaPhone automatically updates the list from PortaBilling® via the API.

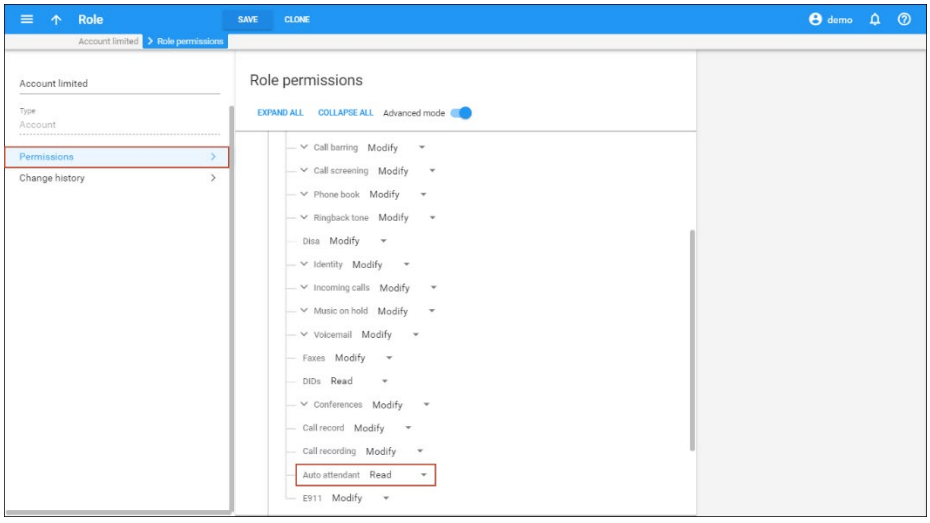


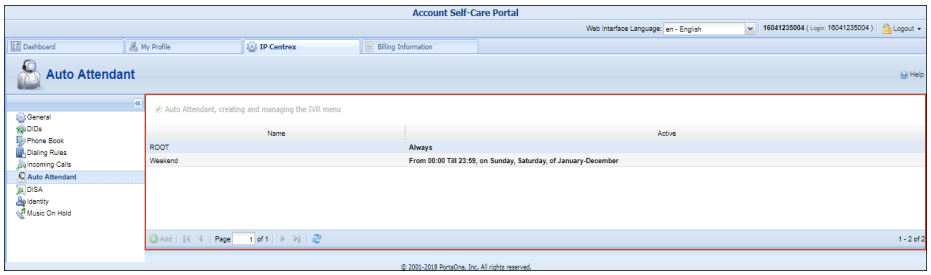
To ensure the extensions list stays up-to date, the app sends periodic API requests to PortaBilling® to refresh it. You define the refresh period along with other parameters on the configuration web portal when you build your app image that you then publish in Google Play / Apple App Store.

This enhancement improves the user experience with your IP Centrex solution.

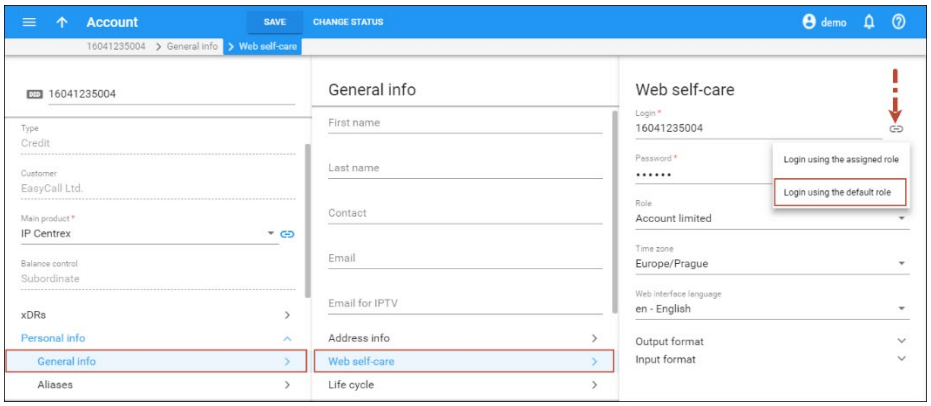
- **Role-based access control for customer / account self-care** – As of this release, administrators use roles to control access to customer / account self-care pages. Roles preserve the permissions of default and custom access levels (ACLs) and are automaticaly assigned to corresponding customers and accounts. It is possible to create new custom roles and manage their permissions as well.

  For example, let's say that customer EasyCall Ltd. wants the account 16041235004 to have read-only access to the auto attendant functionality. An administrator creates the "Account limited" custom role and defines the **Read** permission for auto attendant functionality. On the web self-care panel, the administrator assignes a new role to the account 16041235004. When the account owner enters the self-care portal, they see the auto attendant tab as read only.





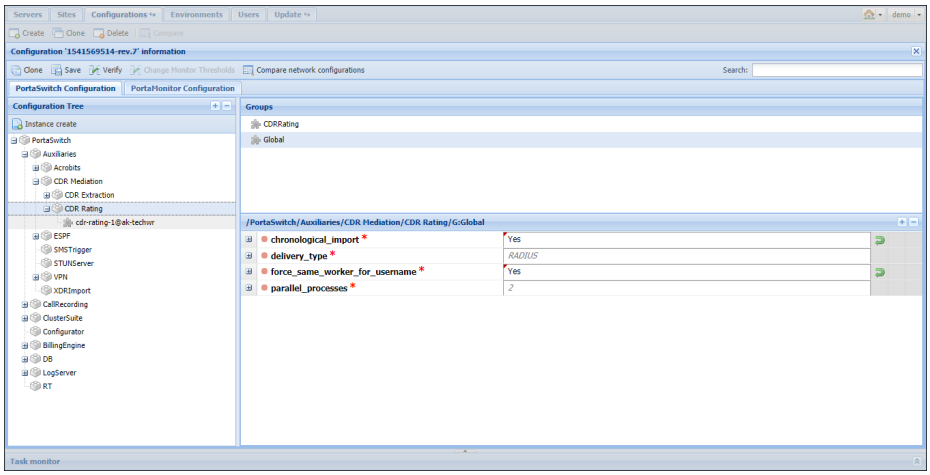

An administrator can log into a customer self-care portal on behalf of the customer, for example, to help with the IP Centrex configuration. If the customer has a custom role assigned to them, the administrator can choose whether to log in with either the custom or the default role.




This enhancement provides the ability to control access to the self-care page for both customers and account owners.

- **Speed up import of CDRs in chronological order** – An administrator can now configure PortaBilling® to chronologically import CDRs in several parallel flows so that the CDRs for several accounts are simultaneously imported.

  To make this happen, an administrator enables **chronological_import** and **force_same_worker_for_username** options and sets the number of workers for the CDR Rating instance on the Configuration server.




When processing a source file with CDRs for multiple usernames, the Rating instance:

- chronologically sorts the CDRs within a collection, based on their time stamp (e.g. connect time for voice calls),
- distributes the CDRs among available workers (two by default), one at a time based on the Username, and
- controls that each worker processes the CDRs with the same Username.

Thus, for each account, the earlier CDRs are rated before the later ones. For example, xDRs for free calls made within a quota are processed earlier than xDRs for charged calls made once a quota is exceeded.

The number of possible parallel processes is only restricted by the processing capacity of your system. The minimum number of these is 1.

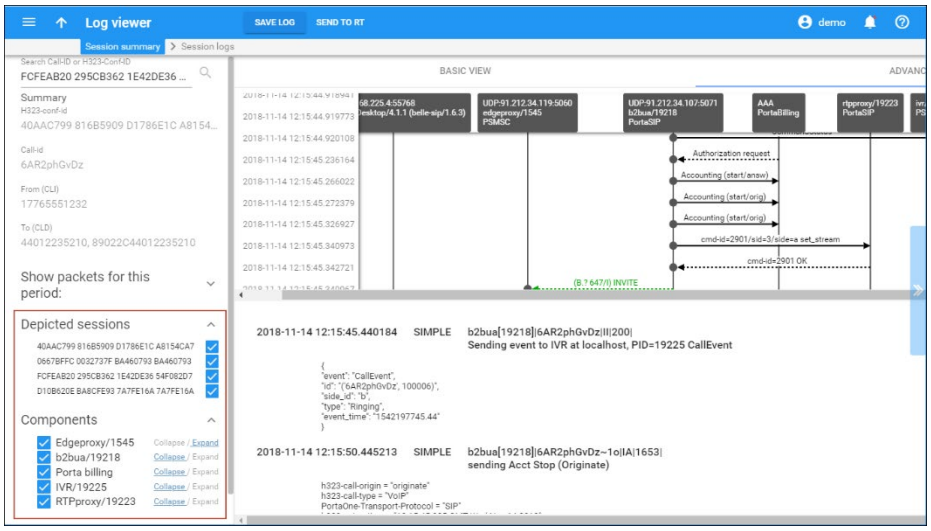
# Web interface changes

- **Filter log by related sessions** – A single session can consist of several subsessions (e.g. a user makes an outgoing call via the Pass-through IVR and then transfers that call to another party. Such a call has several call legs: one to the IVR, another to the destination and one to the transfer party).

  When troubleshooting unsuccessful sessions, an administrator can now filter the required log part from the whole session log (e.g. display only the details related to call transfers).

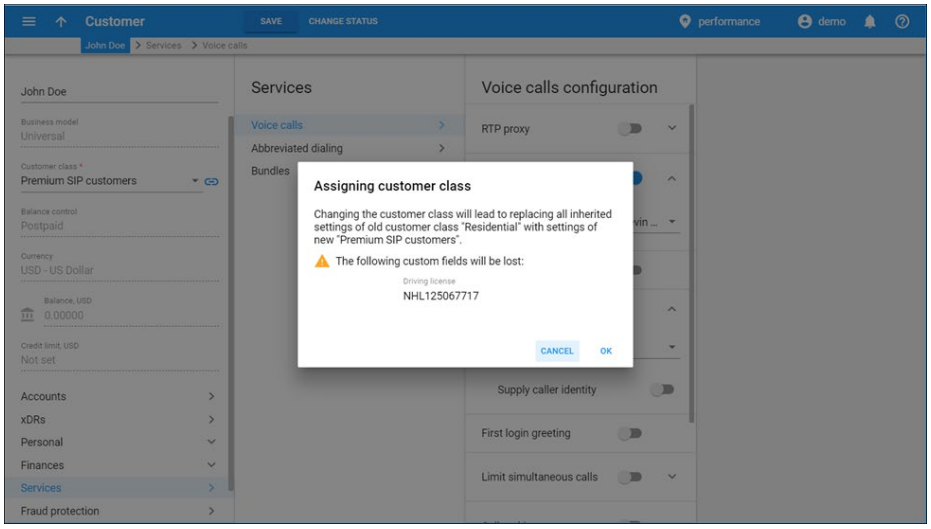
  To make this happen, the administrator switches to the **Advanced view** on the Log viewer page and clears the unnecessary H323-

conf-id in the **Depicted sessions** section. If they want to further refine the data display, they can click the **Collapse** link next to the system component that they are not interested in.




This enhancement facilitates troubleshooting and saves the administrator's time so they can find the root of the issue and fix it quicker.

- **Notification about losing custom field data during a customer class change** – An administrator can change a customer class for a customer (e.g. to apply a different payment collection policy), and now they can be notified about replacing the previous configuration with a new one. If the previous customer class contains custom fields, the administrator also sees a warning that these custom fields will be deleted and all the information stored in them (e.g. the driving license ID) will be lost.



Thus, being timely notified about possible consequences, the administrator can respond accordingly (e.g. reconsider changing the customer class or back up the custom field data somewhere else). This step improves the user experience with the product

# Important upgrade notes

- **Fraud traffic profile as a unified fraud prevention tool** – With this release, spending plans and service usage monitoring profiles (previously known as Fraud traffic profiles) are united into a single **Fraud traffic profile** tool.

  During the update, the system checks which fraud prevention tools were applied to the customers and resellers: spending plans, service usage monitoring profiles or some combination thereof. Based on this data, the system creates new fraud traffic profiles for a customer / reseller that preserve the configuration of the spending plan and / or service usage monitoring profile.

  Fraud traffic profiles receive the name of the spending plan / service usage monitoring profile preceded by a unique prefix (e.g. f_8_5_798) and inherit the currency from the customer they are assigned to.

  The prefix contains information about:
  - the originating entity ("f" – for service usage monitoring profile, "s" – for spending plan, "s" and "f" – for some combination thereof);
  - the unique ID of the originating entity (e.g. 8);
  - the index number received during migration (e.g. 5);
  - the time stamp in milliseconds (e.g. 798).

  For example, customer DEF operates in USD and has an "International calls" service usage monitoring profile assigned. During an update procedure, the system creates a new fraud traffic profile with the name "f_8_5_798_ International calls." The fraud traffic profile inherits the USD currency from the customer.

  There are many possible combinations and the system reviews them during the update procedure to create new fraud traffic profiles. This ensures that each customer, customer class or reseller preserves their configuration after an update.