PORTA ONE

PortaSwitch

New Features Guide

www.portaone.com

Copyright notice & disclaimers

Copyright © 2000–2021 PortaOne, Inc. All rights reserved

PortaSwitch® New Features Guide, January 2021
Maintenance Release 90
V1.90.04

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 90 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.

Support of STIR/SHAKEN standards

The phone number of the caller can be easily altered or spoofed to mask unwanted robocalls (phone spam). The users answer these calls thinking it's from a known caller, for example, their neighbor. To comply with local regulators in the US and Canada, and stop robocalls, service providers can now authenticate outgoing calls and verify incoming calls using Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN). STIR/SHAKEN ensures the authenticity of the calling numbers. With STIR/SHAKEN, users will see the verified V-sign that lets them know they can trust the calling number they see on their phones. If the calling number is not verified, they won't see the V-sign, and they can choose for themselves whether or not to answer.

SIP trunking providers can also sign calls with the STIR/SHAKEN signature and avoid penalty charges for not complying with regulations.

To implement STIR/SHAKEN, service providers perform the following steps:

1. Register with the Policy Administrator on the **Service Provider page** to receive a Service Provider Code Token.
2. Set up an account with an approved certification authority such as TransNexus to obtain a digital certificate necessary to sign the calls with a digital signature.
3. **Configure PortaSwith®** to authenticate and verify calls.

PortaSwith® is integrated with TransNexus, a certification authority and a service provider of authentication and verification services. Contact our **sales team** if you want to use the other certification authority.

Benefits

- Compliance with the local regulations for service providers.
- Users can trust the verified calling numbers and decide whether to answer the other calls.

Let's see how STIR/SHAKEN works for the authentication of outgoing calls and verification of incoming calls.

Authentication of outgoing calls

The service provider is responsible for authenticating all the calls they originate. Since the level of trust in the caller identity may differ, service providers choose the following trust gradation for the calls:

- **Full attestation**. The service provider authenticates the user making the call and confirms they are authorized to use the phone number. For example, the authenticated user makes a call using the phone number allocated by the service provider.
- **Partial attestation**. The service provider authenticates the customer making the call but cannot confirm that the calling party is authorized to use the phone number. For example, a call is initiated by your IP Centrex customer from a non-authorized number.
- **Gateway attestation**. The service provider indicates that they let the call enter on their network, but they cannot verify the call originator. For example, a call is received from an international gateway or a wholesale partner.

Let's consider an example. Mary Smith, your PortaSwitch® user, makes a call to John Doe, a user of your vendor, Panda Telecom. Mary's account is set for full attestation. When Mary calls John, PortaSIP® first authorizes the outgoing call and gets the call signed with a digital signature and then sends the call to Panda Telecom.

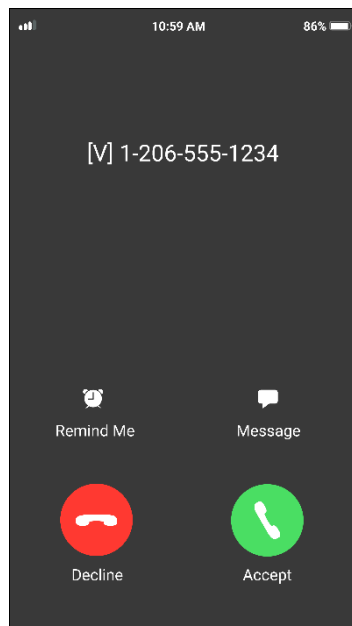The authentication flow for the call looks like this:
- PortaSIP® receives the SIP INVITE request from Mary (**1**).
- PortaSIP® checks the attestation level to determine whether to attest the call (**2**).
- PortaSIP® adds the verified caller identity (P-Asserted Identity) to the SIP INVITE request and sends the request to TransNexus, the authentication service, to receive the signature in the SIP Identity header (**3**).
- TransNexus sends a 302 ("Moved Temporarily") response, which includes the SIP Identity header. This means that a call is signed (**4**).
- PortaSIP® sends the SIP INVITE request with the SIP Identity header to Panda Telecom (**5**).
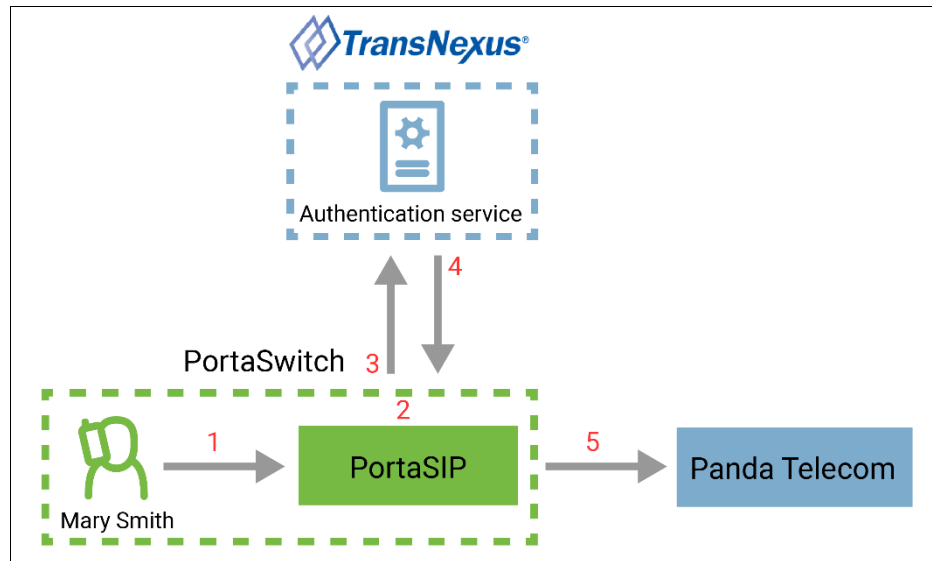
Verification of incoming calls

The service provider is responsible for verifying the calls that enter their network. The service provider passes the Identity header and the digital signature received from the origination service provider to TransNexus for verification.

Let's say, the account of Mary Smith, your PortaSwitch® user, is configured to verify all the incoming calls. When John Doe (the user of Panda Telecom service provider) calls Mary Smith, PortaSIP® first verifies the incoming call from John in TransNexus. If the call passes the verification, Mary sees that she can trust the calling number: she sees [V] sign before the phone number.

The verification flow for the call looks like this:

- PortaSIP® receives the SIP INVITE request, which includes the SIP Identity header and the signature (**1**).
- PortaSIP® sends the SIP INVITE request to TransNexus for verification (**2**).
- TransNexus responds PortaSIP® that verification is successful (**3**).
- PortaSIP® adds [V] sign before the calling number and sends the incoming call to Mary Smith (**4**).
- Mary sees [V] 12065551234 meaning that the call from John is verified.
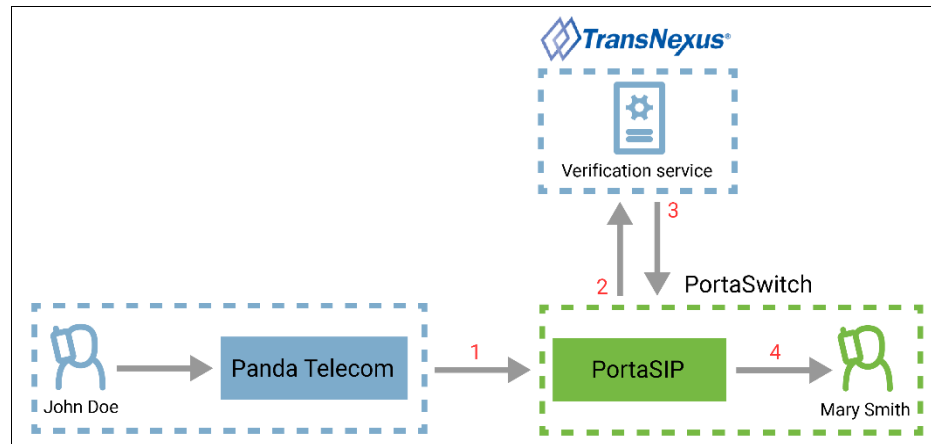
Note that the verification sign [V] is only displayed for users if the calling phone number has the full attestation level.

Configuration

To configure the outgoing call authentication in PortaBilling®, the administrator:

1. Updates the service policy that is assigned to the Internal vendor connection and connections of the US and Canada vendors that support STIR/SHAKEN:
   - Opens the **Service policy** > **Attributes** > **SIP headers**.
   - Selects the checkbox for **Stir signature required** option and turns on the toggle switch.
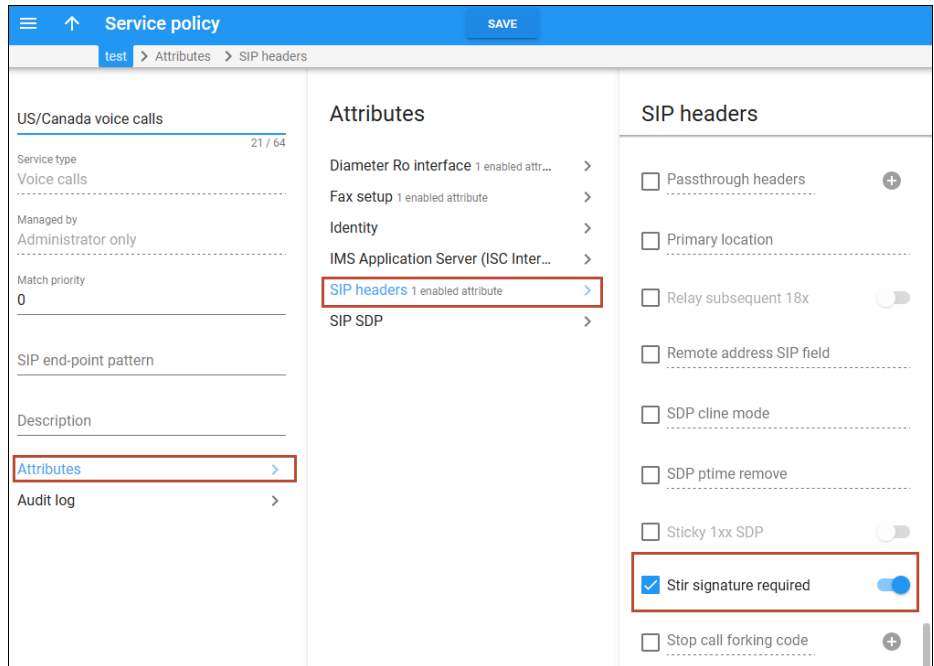
2. Configures the **Override identity** feature for outgoing calls:

- Opens Mary's **Customer** > **Services** > **Voice calls** > **Outgoing calls**.
- Turns on the toggle switch to enable the **Override identity** feature.
- Specifies 12060655556 in the **Identity** field.
- Sets the **Attestation level** to **Full attestation**.
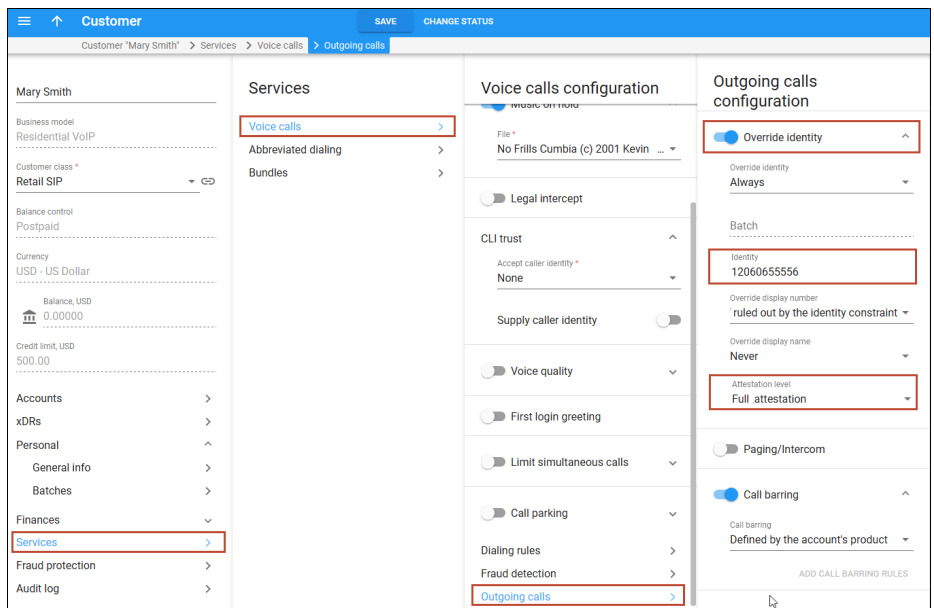
To configure the incoming call verification in PortaBilling®, the administrator:

- Opens Mary's **Product** > **Services** > **Voice calls** > **Incoming calls**.
- Turns on the toggle switch to enable the **Perform caller verification** feature.
- Sets the **Display name indicator** as **Caller name and SIP headers**.
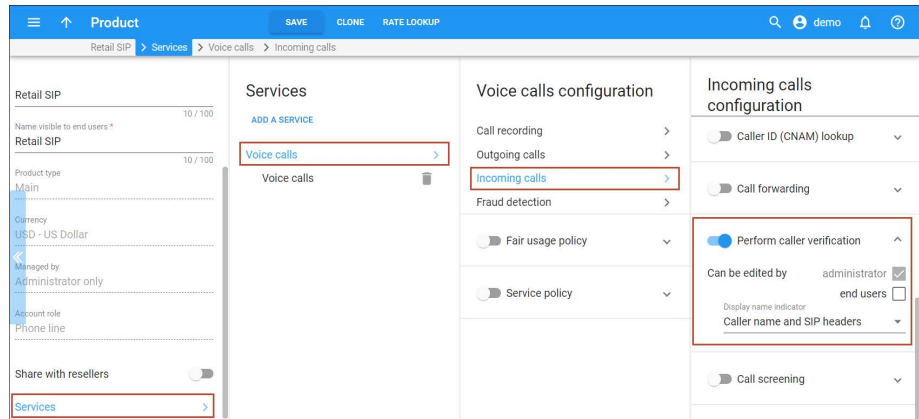

Integration with Pharos CIG

With PortaBilling® as the Online Charging System (OCS), mobile virtual network operators (MVNO) can offer a full range of mobile services to their customers. PortaBilling® supports 2.5/3G and 4G mobile networks and uses Diameter (Ro) as the main protocol for online charging. Since the CAMEL protocol is the main protocol used for real-time charging in 2.5 and 3G networks, additional gateway is required to convert the CAMEL requests to Diameter (Ro) requests.

With this release, PortaBilling® is integrated with one more gateway that converts the CAMEL requests to Diameter (Ro) requests and vice versa – the Pharos CIG (Charging Interworking Gateway). With the Pharos CIG, PortaBilling® supports real-time charging for domestic and roaming voice calls, SMS, and **USSD**.

The Pharos CIG is deployed within a service provider's network and acts as a mediation component between PortaBilling® and a mobile operator's network. The Pharos CIG communicates with the MSC (Mobile

Switching Center) using the CAMEL protocol and then converts the CAMEL to Diameter (Ro) to communicate with PortaBilling®, and vice versa.
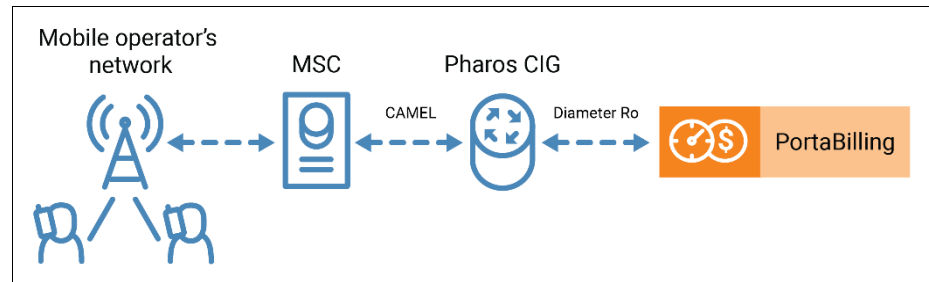
This is how it works:

Let's say you are the MVNO in South Africa who provides domestic/roaming voice calls and SMS to subscribers. John Doe is your subscriber. When John Doe makes a call to a destination 27115557122, South Africa, the MSC performs the call authorization in PortaBilling® to verify that John Doe has sufficient funds to call this destination. The MSC sends the authorization request to PortaBilling® via the Pharos CIG using CAMEL protocol. The Pharos CIG receives the authorization request from the MSC, converts it from CAMEL to Diameter (Ro) and sends this request to PortaBilling®. PortaBilling® locks in the funds to cover the initial period of the call and replies to the Pharos CIG with a confirmation message using Diameter (Ro). The Pharos CIG receives the reply from PortaBilling®, converts it from Diameter to CAMEL, and sends it to the MSC. When the initial period of the call is over, the MSC sends requests to lock in the funds for the subsequent periods. When John Doe finishes the call, the MSC sends a request to PortaBilling® to inform it that the call is over. PortaBilling® creates an xDR record for this call.

You can find the configuration details and the workflow for roaming voice calls and SMS services in **PortaBilling® Administrator Guide** in the **Real-time billing for roaming services** chapter.

This integration allows service providers to run MVNO in 2.5 and 3G networks and offer a full range of mobile services to their customers using another CAMEL to Diameter gateway.

Other features and enhancements

Add exceptions when passing number portability parameters in outgoing calls

In certain countries, such as the Dominican Republic, vendors can drop calls to numbers that cannot be ported (like toll-free or emergency numbers) if they contain the number portability parameter **npdi** in the incoming INVITE request. As a result, the end-users may fail to reach toll-free or emergency numbers. To avoid dropped calls to such numbers, you can skip adding the number portability parameter **npdi** into calls to specific destinations and numbers.

With this release, to add the number portability parameter **npdi** to outgoing calls to domestic destinations, the administrator needs to add these destinations or numbers to the `Number_Portability table` and specify the "**=**" value in the `origin` field. For example, for the Dominican Republic, the administrator needs to add prefixes: 1809, 1829, and 1849. For outgoing calls to destinations and numbers that are not present in the `Number_Portability table`, PortaSIP® adds no number portability parameters.

To skip adding the number portability parameter **npdi** in calls to a certain destination or number (for example, 1809200 destination for toll-free numbers), the administrator adds this destination or number to the `Number_Portability table` and specifies the "**!**" value in the `origin` field.

For calls to ported numbers (contained in the database of local ported numbers in PortaSwitch®), PortaSip® keeps adding number portability parameters **npdi** and **rn** (routing number) to the outgoing INVITE request.

This enhancement allows the service providers to comply with local regulations and ensure that mission-critical calls and calls to toll-free numbers reach the called party.

This is how it works:

Let's say the administrator enables local number portability functionality in PortaSwitch® and imports the list of ported numbers to the PortaSwitch® database. The administrator also enables PortaSIP® to pass the number portability parameters in the outgoing INVITE requests. Then the administrator adds particular numbers and destinations to the `Number_Portability table`.

destination	origin (routing number)	action
1809, 1829, 1849	**=**	Regular domestic numbers. PortaSIP® adds **npdi** parameter to outgoing calls.
1809200	**!**	Toll-free numbers. PortaSIP® adds no **npdi** parameter to outgoing calls.
18295557777 (Claro)	**180972**62222 (Viva)	The number is ported. PortaSIP® adds **npdi** and **rn** parameters to outgoing calls.

The service provider's customer, John Doe, makes a call to **1809**2555000. PortaBilling® looks up the destination in the PortaSwitch® database using the longest match and finds the **1809** destination added as a regular domestic not-ported number. Thus, PortaSIP® passes a number portability parameter **npdi** in the outgoing INVITE request like this:
```
INVITE sip:18292555000;npdi=yes@190.123.72.1:5060;user=phone
SIP/2.0.
```

Then John Doe makes a call to **1809200**5550, a toll-free number. PortaBilling® looks up the destination in the PortaSwitch® database using the longest match and finds the **1809200** destination added as an exception. Thus, PortaSIP® does not pass number portability parameters in the outgoing INVITE request:
```
INVITE sip:18092005550@190.123.72.1:5060;user=phone SIP/2.0.
```

The next call John Doe makes is to **18295557777**. This number originally belonged to the mobile operator Claro, but has been recently ported to another operator, Viva. PortaBilling® looks up the number in the PortaSwitch® database using the longest match and finds **18295557777** added as a ported number that now belongs to Viva. For this reason, **180972**62222 must be used for further routing, and the call must be charged according to Viva's rates. Thus, PortaSIP® passes number portability parameters in the outgoing INVITE request like this:
```
INVITE
sip:18295550000;rn=18097262222;npdi=yes@190.123.72.1:5060;user=
phone SIP/2.0.
```

Charging for USSD sessions

PortaBilling® now supports charging for USSD sessions for service providers that launch MVNOs in a 2.5/3G network using Pharos Charging Interworking Gateway (Pharos CIG).

Unstructured Supplementary Service Data (USSD) requests allow mobile phone users to request information or perform various actions by dialing short codes. For example, a user can dial *136# to check the current balance or *136*4# to change the package.

The advantage of the USSD services is that they require neither Internet access nor a smartphone. With USSD requests, MVNOs can provide services that are easy to access from any mobile phone.

Usually, USSD requests are free of charge, but service providers may charge users for some of them (e.g., USSD requests for activation of premium features, accessing banking services, or receiving various content such as news, currency exchange rates, weather forecasts).

Specifics

NOTE: To enable charging for USSD sessions, the PortaBilling® integration with the Pharos CIG (Charging Interworking Gateway) must be configured.

The USSD sessions charge is time-based. For example, a South African MNO MTN uses a twenty-second interval for USSD sessions charging, meaning that the users are charged $0.2 for every 20 seconds of a USSD session. During a session, every 20 seconds PortaBilling® receives a new Diameter request from the Pharos USSD gateway. This interval is configured in tariff rates in PortaBilling®. Every 20 seconds of the session show up as a separate xDR in PortaBilling®.

Let's consider examples for 2 types of USSD sessions:

1. Sessions with menu options. For example, John Doe wants to check the currency exchange rates. He dials *102*3#. A new USSD session starts and John receives a USSD message with a menu with various options ("News, press 1", "Currency exchange rates, press 2", "To go to the main menu, press 0" etc.). John dials 2 and receives a USSD message with exchange rates. Then he decides to also check the news. John dials 0 to go back to the main menu and dials 1 to check the news. After that, John presses the "Close" button to terminate the session. The duration of the session is 45 seconds. From the session initiation, the Pharos USSD gateway has sent to PortaBilling® three Diameter requests of 20 seconds each, so the total cost of this USSD session is $0.2*3=$0.6.

2. Sessions without menu options. Let's say John Doe dials *102*444# to change the current package to "Basic," the cheaper one. John receives a USSD message that his package was successfully changed. He presses the "Close" button (no other actions are available). The service provider charges John Doe $0.2 for this request as if it was a twenty-second session.

Benefits

With this enhancement, service providers operating at markets where USSD services are in demand can monetize these services.

Configuration

To configure charging for USSD sessions, do the following:

1. Go to the **Configuration server** > **BillingEngine** > **Custom** group:
   - for the **Custom.IniOptions** attribute, add the following string:
   [Pharos]RoServiceContexts=[*the value of the Service-Context-Id AVP that is sent in the Diameter request for USSD*].
   For example, for an MVNO launching in the MTN network, this string looks as follows:
   [Pharos]RoServiceContexts=010.655.02.ussd@mtn.co.za;
   - for the **Custom.LoadAdapterModules** attribute, specify:
   pharos=Porta::BE::M::Adapter::Pharos.
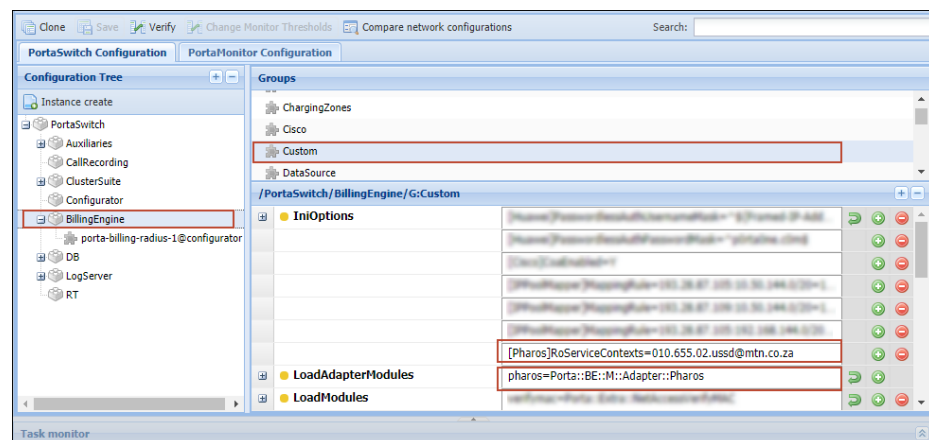
2. Go to PortaBilling®:
   - Create a separate service to charge for USSD sessions (select **Voice calls** as a service type).
   - Add the available USSD short codes (e.g., *101#, *102*3#) to the list of destinations in PortaBilling® as custom destinations.
   - Add rates for each short code to the vendor tariff (e.g., Destination – *101#, Rate – $0; Destination – *102*3#, Interval – 20 seconds, Rate – $0.3).

- Create a customer tariff to charge for USSD sessions. Create a rate for each short code (e.g., Destination – *101#, Rate – $0; Destination – *102*3#, Interval – 20 seconds, Rate – $0.6).
- Open the mobile service product and add the USSD service on the **Services** page.
- Open the **Usage charges** page for the product and add a record with the following access code: OUTGOING.SI[*the number specified in the value of the* **Service-Identifier** *AVP in the Diameter request for USSD*].
  For example, if you configure an MVNO launching in the MTN network, the access code looks as follows: OUTGOING.SI120.

  Next to the **Access code** field, select the created customer tariff for USSD charges.

- Create a voice calls service policy, enable the **Rise MSCC result code** attribute for it, and assign this service policy to the product (or an account).