PORTA ONE

PortaSwitch

Configuration Server Web Reference

MAINTENANCE RELEASE 80

www.portaone.com

Copyright notice & disclaimers

PortaSwitch® Configuration Server Web Reference, October 2019
Maintenance Release 80
V1.80.01

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

This document provides a general overview of the web interface for the PortaSwitch® Configuration server.

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 that occur in-between minor 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`.

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 taking the action described here.

Tips provide information that might help you solve a problem.

Gear points out that this feature must be enabled on the Configuration server.

Trademarks and copyrights

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

Document objectives

This publication provides technical information on the PortaSwitch® Configuration server's web interface usage. It is designed for use either in conjunction with other materials or as a standalone reference.

Audience

The target audience of this document is comprised of system administrators, VoIP engineers and system operators who will be managing your PortaSwitch® system via the web interface of the configuration server.

Hardware and software requirements

Client system recommendations

- **OS:** MS Windows 7 or above, Linux/BSD, macOS Sierra (version 10.12) or above.
- **Web browser:**
  - Google Chrome 70 or above, Mozilla Firefox 63 or above.
  - JavaScript and cookies must be enabled.

- **Spreadsheet processor:** MS Excel, OpenOffice Calc, LibreOffice Calc, Google Sheets.
- **Display settings:** A minimum screen resolution of 1366 × 768.

What is new in Maintenance Release 80?

Added:

- The **UI Plugins** chapter.

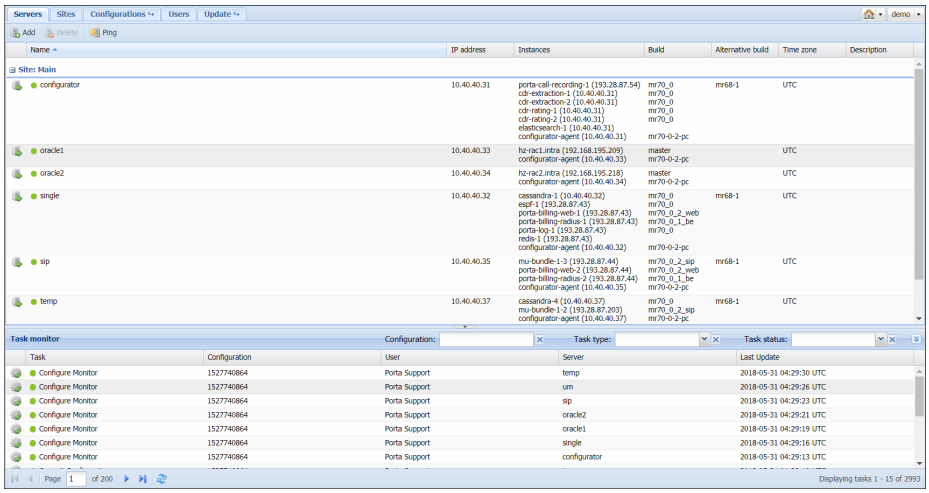
1. Introduction

Login to the Configuration server interface

Open the Configuration server web interface in a browser (**https://<configuration_server_name>:8700** by default) and type in the username and password which were provided to you.

The web interface of the configuration server contains:

- Tab selector
- Action buttons
- Toolbar
- Data table
- Task Monitor



Tab selector

In the upper left-hand corner, there are four main functional tabs and three additional tabs that allow you to manage the different elements of your PortaSwitch® system. The main functional tabs are: **Servers**, **Configurations**, **Users** and **Update**.

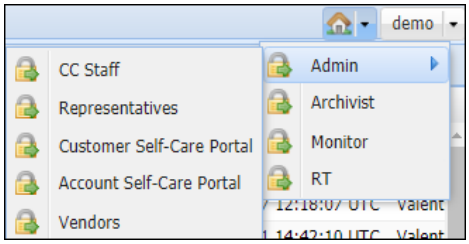
The **Environments** tab becomes visible when you open the **Configurations** tab.

The **Custom**, **Deposit and UI Plugins** tabs become visible when you open the **Update** tab.

The definitions of and available functionality for each tab are explained in the following sections. Note that not all users have complete access to the entire set of tabs.

Action buttons

The  **Home** icon in the right-hand corner contains a menu with shortcuts to all the other PortaSwitch® interfaces:



The **Admin** button – shortcut to the administrator web interface of PortaBilling:

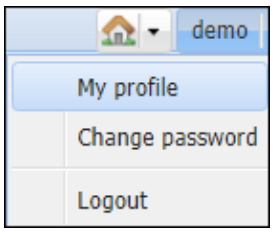
- **CC Staff** – Customer care staff interface.
- **Representatives** – Interface for your sales agents or distributors.
- **Customer Self-Care Portal** – Interface for customers (owners of IP Centrex environments).
- **Account Self-Care Portal** – Interface for account owners (end users).
- **Vendors** – Interface for your termination partners.

The **Archivist** button takes you to the web interface where you can configure backup for the most critical data on your installation.

The **Monitor** button takes you to the web interface of the monitoring facility for your PortaSwitch installation.

The **RT** button takes you to the web interface of the trouble tickets system where you can view the list of your requests and perform the needed actions (e.g. close, update or create a new ticket).

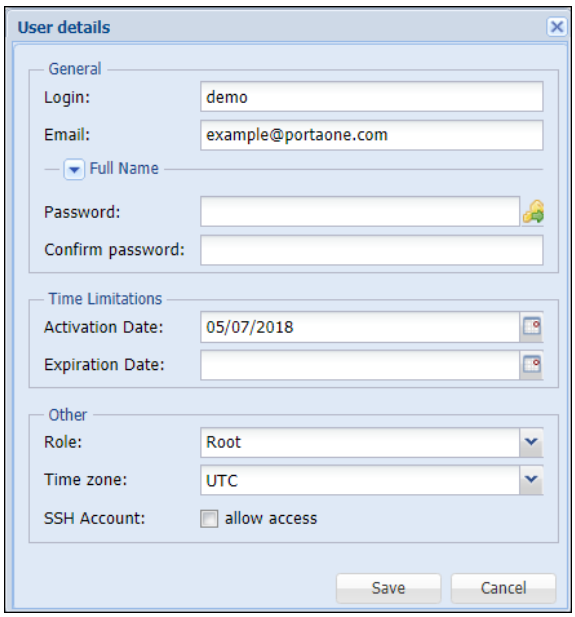
Other buttons in the upper right-hand corner allow you to perform a given action, irrespective of the current context.



The **Change password** button allows you to change the password for the current user.

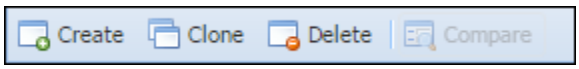
The **Logout** button terminates your current session on the web interface.

The **My profile** button allows you to fill in information about the currently logged-in user:



Toolbar

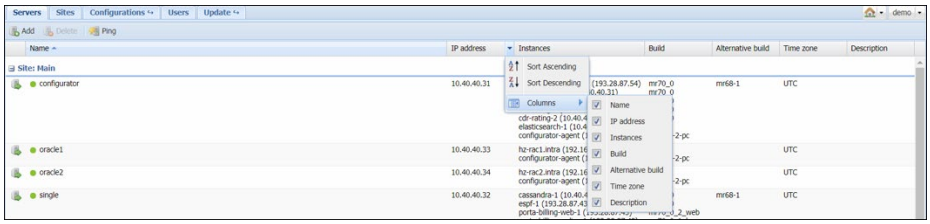
The Toolbar contains buttons that allow you to perform specific operations with the items displayed in the table below.



Item table

The Item Table is your main working area, since it contains the items that you will edit.

You can change the number of columns and sort them in ascending or descending order by clicking your mouse on the field name of any of these tabs. If you point your mouse at the column heading you will see a triangle; click on it to see the menu where you can sort items and add or remove columns by selecting or clearing corresponding check boxes.

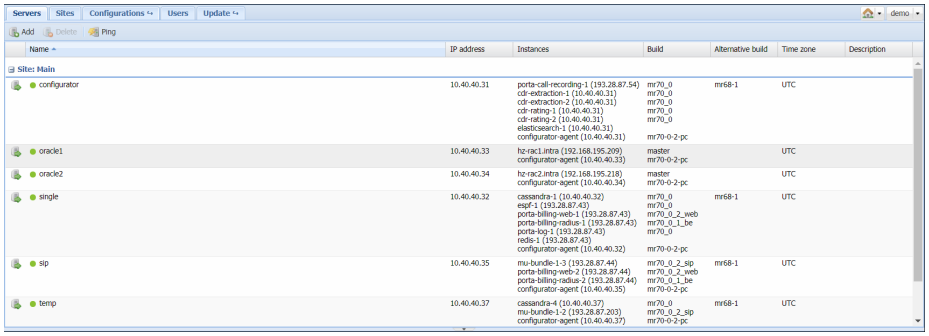


At the bottom of the page, you can see the task monitor illustrating which tasks were performed. You can see which user performed the task, the server on which the task was performed and the time of the last update. See the **Task Monitor** section for detailed information.

2. System management

Servers

The information on the **Servers** tab shows all the servers that are part of your installation.



Field	Description
Name	The name of the server.
IP address	The internal IP address of the server – this address is used on the internal LAN to manage the server from the configuration interface.
Instances	Shows all instances – services that run on your server (e.g. "web interface" or "SIP server") and are assigned to a specific server.
Build	The current software version which is installed and used on the server.
Alternative build	Another software version currently installed on the server (on the inactive partition); a rollback to this version is possible. "N/A" means that the alternative partition does not contain any data.
Time zone	The time zone in which this server is operating. In order to provide optimal system response time for your online users, PortaBilling® only performs resource-intensive calculations (such as creating statistics / invoices) during the preconfigured "off-peak" period. This field specifies the time zone in which the "off-peak" period is configured.
Description	A short description of the server. This field is optional.

An indicator near the name of a server shows whether a specific server is reachable (green light) or unreachable (red light).
The **Servers** page provides the following activities:

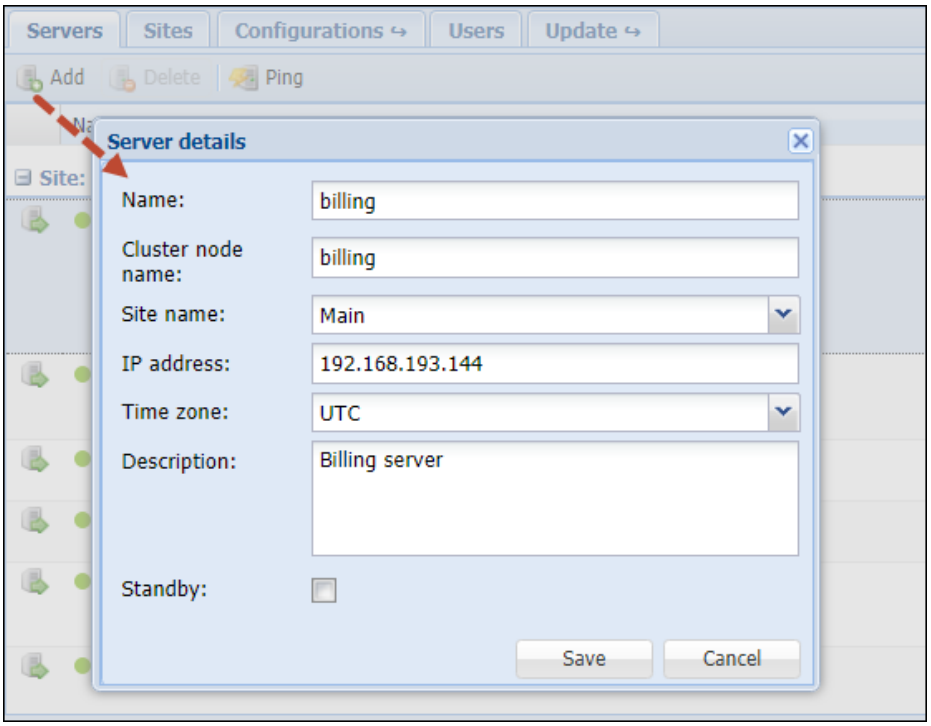
Field	Description
Add	Allows you to add more servers. You will see a dialog box where you should enter the name of the server, its IP address, a short description and specify a time zone; then click **OK**.
Delete	Allows you to delete the selected server.
Ping	Allows you to check the availability of the server. Just click on the **Ping** button and the Configuration server will attempt to verify that it can connect to this server and that the server responds to management commands. If you see a green light, the server is available; if red, then it is not available.

Add / edit a new server

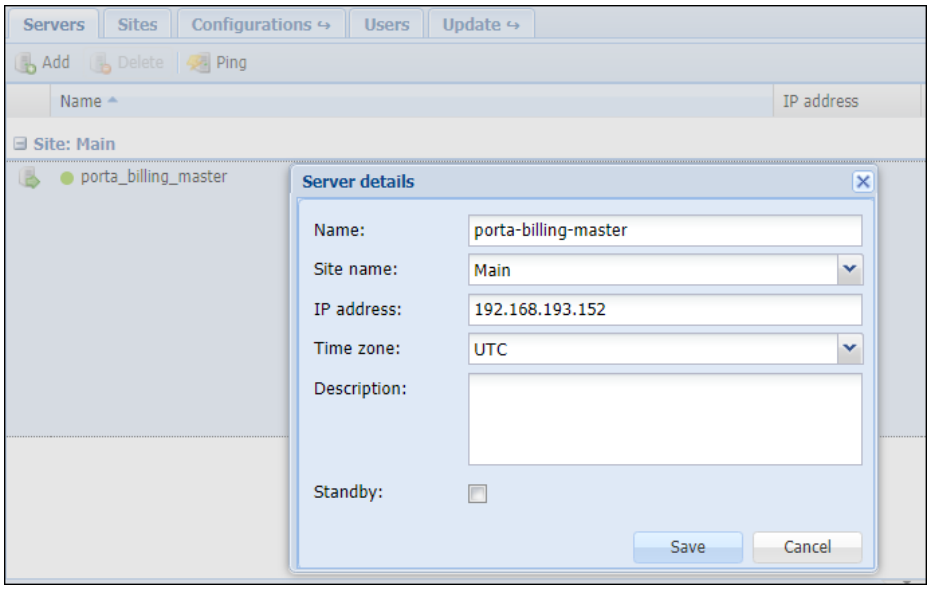
Prior to adding a new server, make sure you have installed the PortaSwitch® software on it using the provided PortaSwitch® installation ISO files.

To add a new server, click the **Add** button in the toolbar and fill in the information about this server:

- **Name** – Type in the new server's name. To avoid confusing the system, do not use a name that begins with "porta-".
- **Cluster node name** – This is the internal name for a server that's part of a cluster. By default, it equals the name of the server. You can only define it when adding the server.
- **IP address** – When adding a server to the installation on this page, an IP is specified. This IP is automatically considered internal, so it (and its NIC) becomes read-only in the Network configuration UI.
- Select the site where the server is located, a time zone in which this server is operating and its description.



To edit an existing server's attributes, double-click on the row that has the server you want to modify.

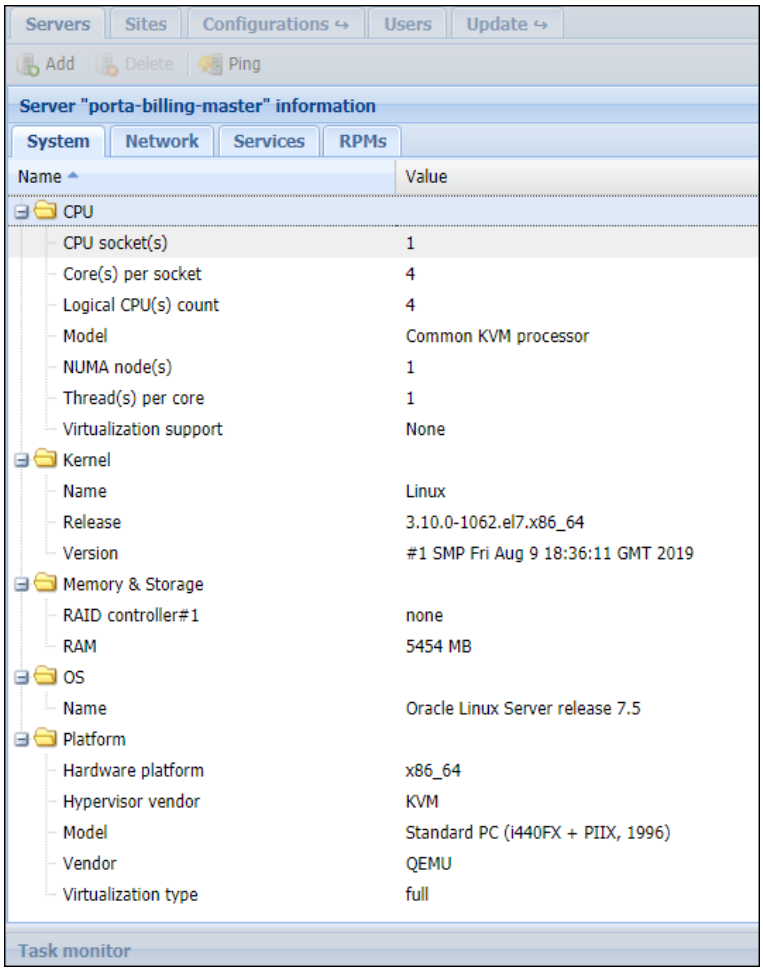


Additional server configuration

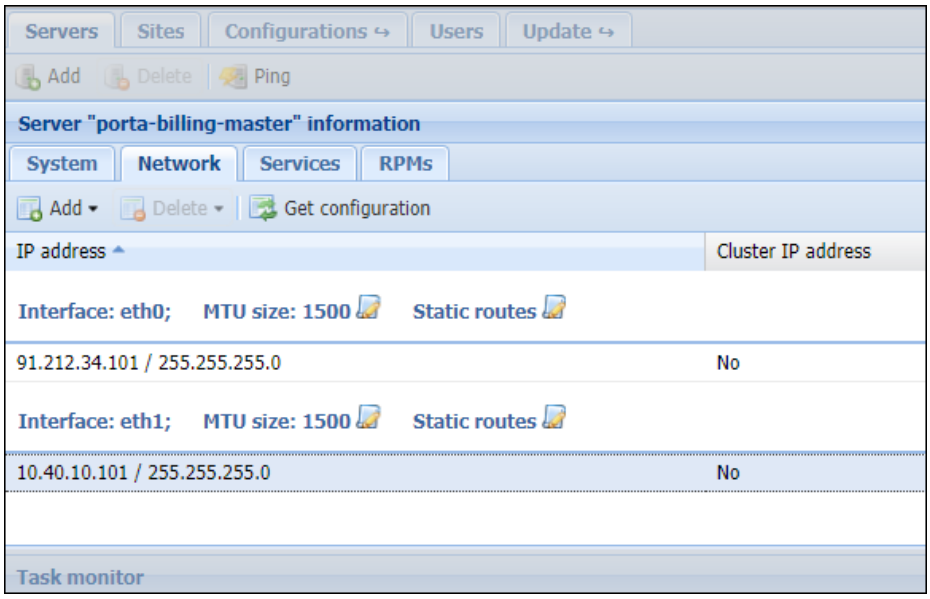
When clicking the **Server Information** button, an additional block opens. This block contains several tabs with different server properties.

You can switch between these tabs to access the corresponding information.

The **System** tab displays basic hardware and software information about the selected server:



The **Network** tab shows all the IP addresses configured for the selected server.



They are grouped by network interface. The following columns are shown:

- IP Address
- Cluster IP address (specifies if this IP address is dedicated to a cluster)

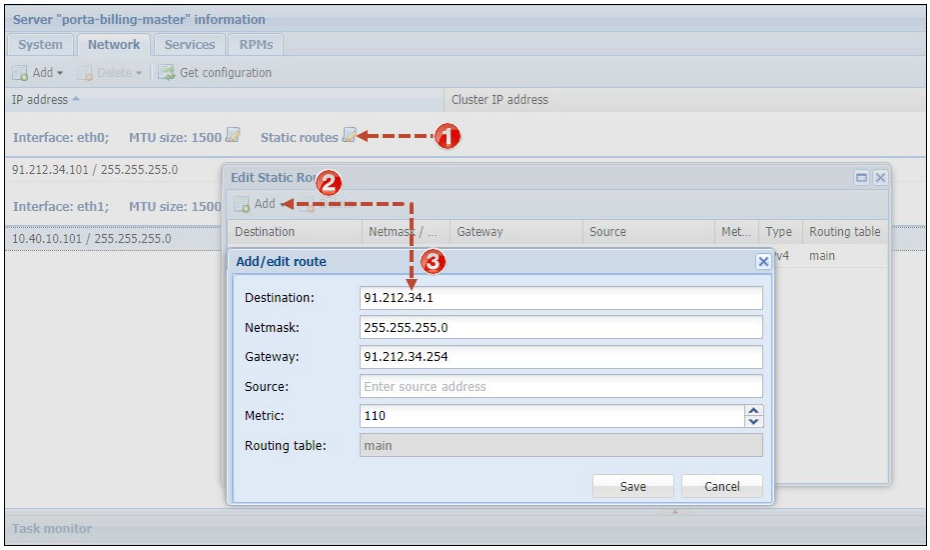
To change either the IP address and / or the subnet mask, just double-click on the specific list element. Edit the parameters in the pop-up window and then press OK.

NOTE: Network interface with internal IP cannot be modified.

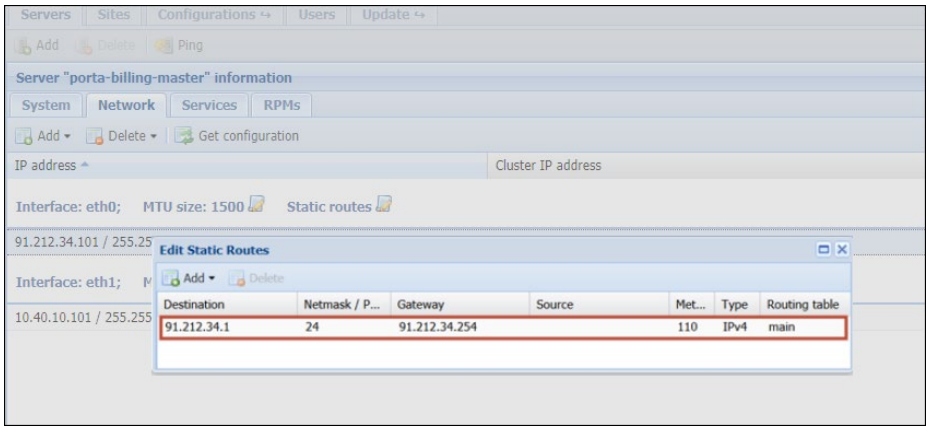
The **Add** button in the toolbar allows you to add a new IP address to a network interface (only those network interfaces that do not have an internal IP address are available) or to add virtual interfaces.

To add and / or modify static routes for a specific server, click the **Static routes** icon.

To add a new static route, click the **Add** button and select the route type (IPv4, IPv6). Specify the required parameters in the pop-up window and click **Save**.



To change the parameters later on, double-click on the row of the static route you wish to modify.



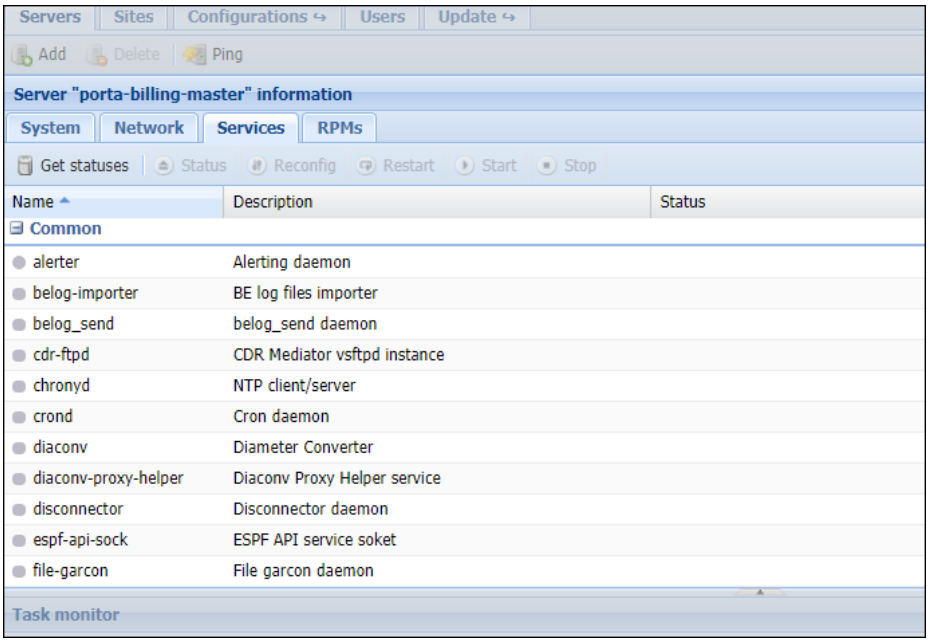
NOTE: To effect changes in the network interface configuration, you have to apply a new configuration on the **Configurations** tab.

The **Network** page provides the following:

Field	Description
Add	Allows you to add a new IP address to a network interface or add virtual interfaces (VLANs for trunking) and / or network bonding (link aggregation).
Delete	Allows you to delete the selected IP address (not available for internal IP addresses).

Get configuration	Gathers information about current network configurations from all servers and updates block content accordingly. **NOTE**: Any changes made on the **Network** tab without applying a new configuration will be lost.

Using the **Services** tab you can control the services that are located on the selected server.

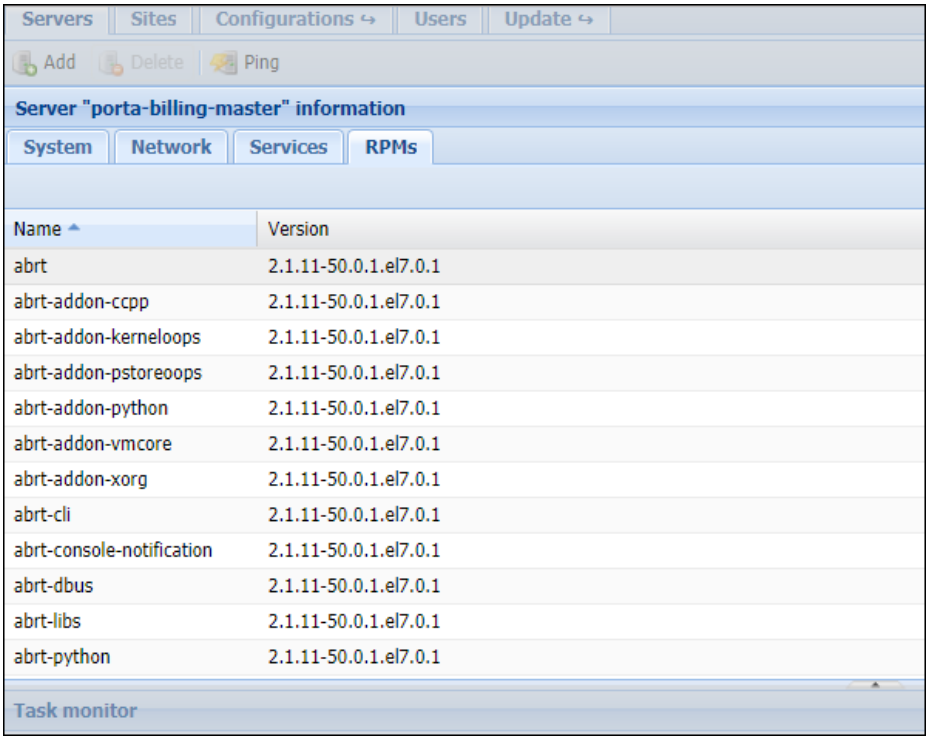


The **Services** tab provides the following activities:

Field	Description
Get statuses	Updates and shows the statuses of *all* services on the server.
Status	Updates and shows the status of the currently selected service.
Reconfig	Re-reads certain configuration parameters without an actual restart.
Restart	Restarts the currently selected service.
Start	Starts the currently selected service.
Stop	Stops the currently selected service.

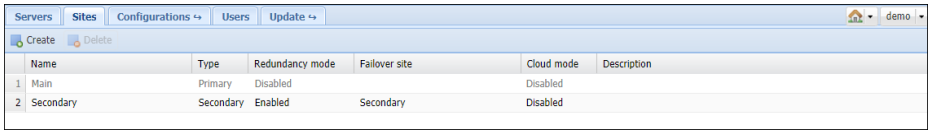
Services are grouped by instances created on the server. The top **Common** group contains general services.

The **RPMs** tab displays RPM packages installed on the selected server.



Sites

The **Sites** tab displays information about all the sites configured within your installation and enables you to manage them. Every installation has a default main site. It is read-only and cannot be either modified or deleted.



Field	Description
Name	The name of the site.
Type	Defines whether it is the main or secondary site. The main site is read-only and cannot be removed.
Redundancy mode	Defines whether the secondary site has been defined as redundant.

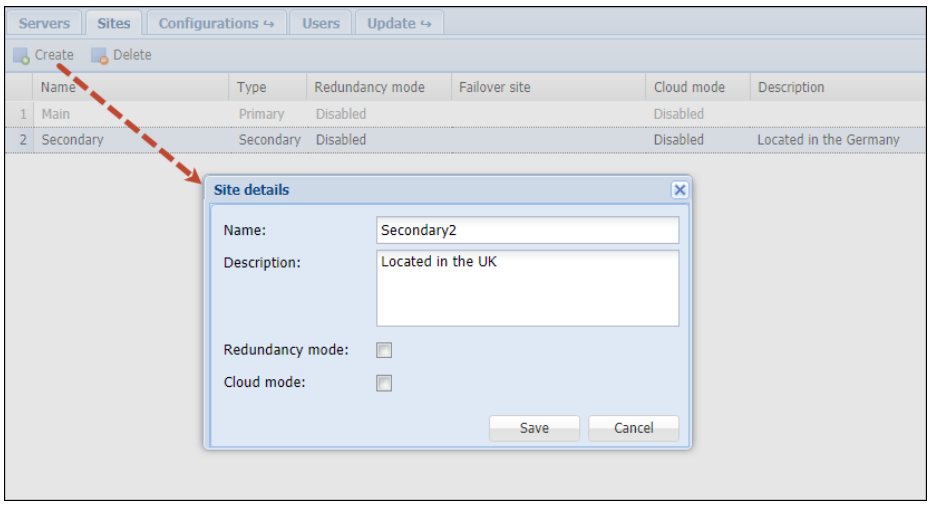
Failover site	Shows which site serves as the failover for a given secondary site. Only secondary sites that have billing instances and stand-by database servers deployed can be selected as failover ones.
Cloud mode	Defines whether the site's servers and instances are configured in the cloud.
Description	A short description of the site. This field is optional.

The **Sites** page provides the following activities:

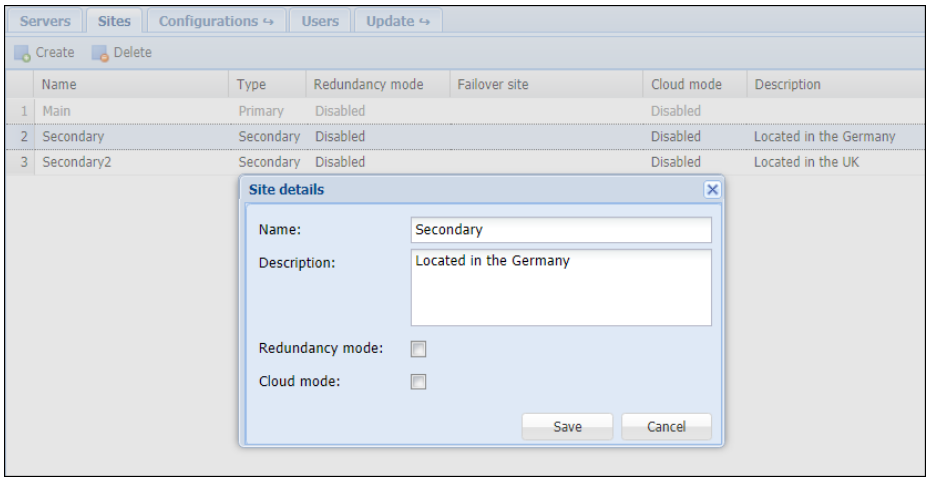
Field	Description
Create	Enables you to create a new site.
Delete	Enables you to delete an existing secondary site. Note that prior to deleting a site, you must reassign its servers to another site.

Add / edit a new site

To introduce an extra degree of reliability within the network and its applications, you can organize the servers into sites. To add a new site, click the **Create** button in the toolbar and then type in the site's name and description. If you manage servers in a cloud, enable Cloud mode for the site.



To edit the attributes of an existing site, double-click on the row of the site you wish to modify.



Redundancy mode

For all of your installation's secondary sites to remain operational when the main site is unavailable, designate one of them as redundant and let the other sites initiate failover to it. To do this, enable the **Redundancy mode** option for the secondary site that contains instances of PortaBilling® and a stand-by database. The system will check this site's configuration and define it in the **Failover site** field.

NOTE: The site, which contains instances of PortaBilling® and stand-by database, can only be made to failover to itself.

Enable the **Redundancy mode** option for other secondary sites and select the previously configured site in the **Failover site** field.

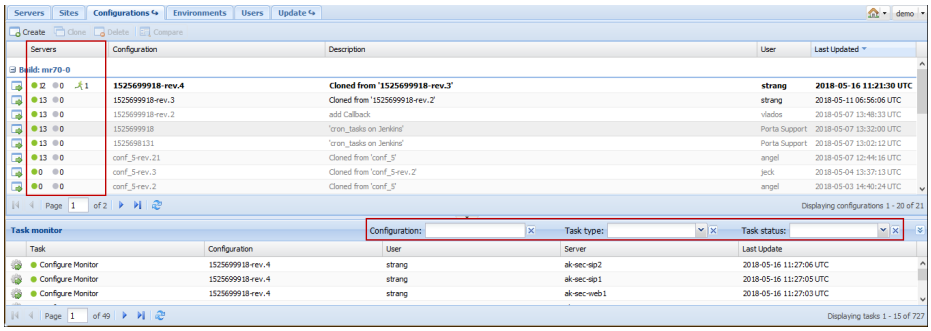
Apply the new configuration to save the changes.

Configurations

This tab allows you to manage the configurations used in your PortaSwitch® system (each row represents a configuration tree).

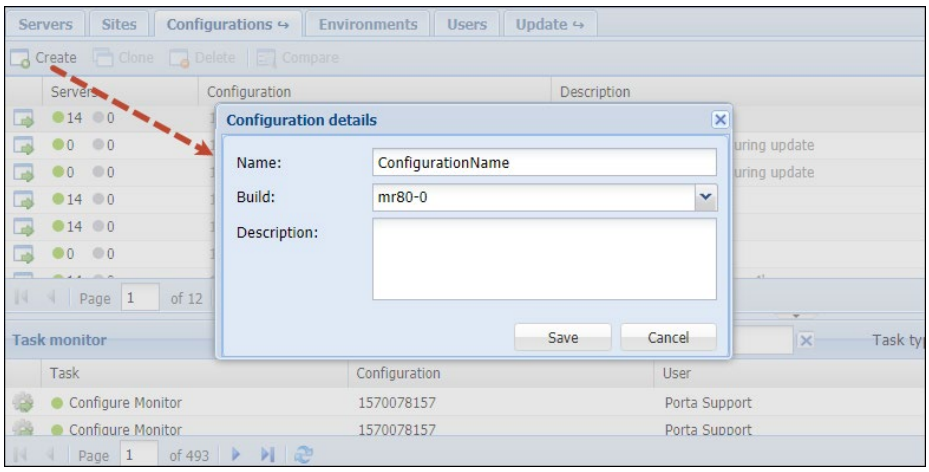
The existing configurations are marked as follows:

- "**active**" (i.e. current) is **bold black**.
- "backup" (i.e. previous) is black.
- "inactive" (i.e. old / new) is grey.



Field	Description
The icon	The configuration information. Click the icon to open the configuration information page.
Servers	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 involved servers. When you click the succeeded or failed indicator those tasks are automatically displayed in the **Task monitor** window.
Configuration	The name of the configuration.
Description	A short description of the configuration. This field is not mandatory.
User	The user who performed the configuration.
Last Updated	The time when the configuration was last edited.

You can create a new configuration by clicking the **Create** button, typing in its name and description and choosing which software version it applies to.

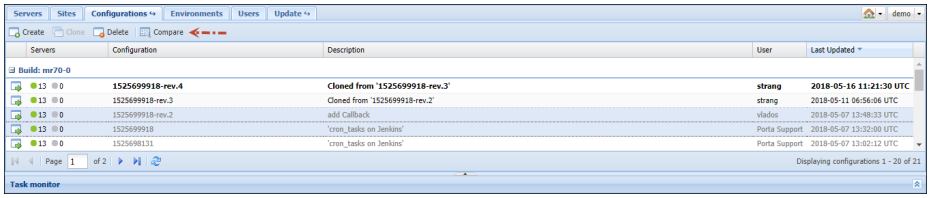


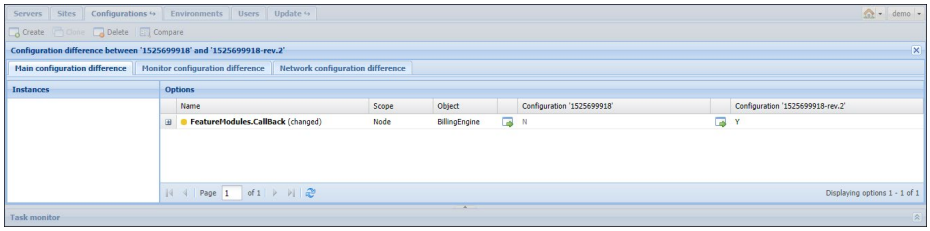
If the configuration already exists, you can edit its description by double-clicking on it.

You can clone the configuration by clicking the **Clone** button (to clone a configuration means to copy it), or delete it using the **Delete** button.

You cannot change or delete the active (currently applied) or the backup (previously used) configurations. This is to ensure that there is always a "stable" configuration you can use for rollback. You can open such a configuration for review using the **Configuration Details** button, or you can create a new configuration as its exact copy (and then edit this new configuration) by using the **Clone** button.

You can easily compare two configurations and see the differences between them. Choose two configurations by holding down the **Ctrl** button on your keyboard, and then click the **Compare** button which will become highlighted above.

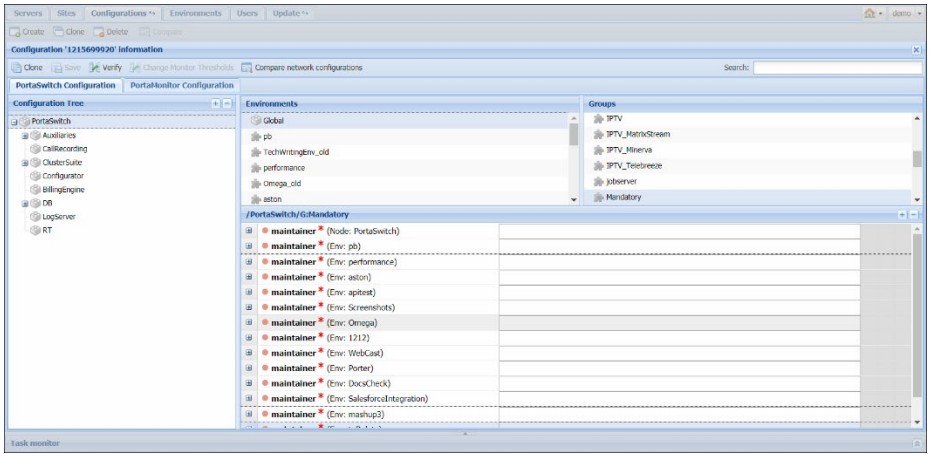




Click the **Configuration Details** button for the required option of the corresponding configuration to open it in the configuration editing mode. Bear in mind that you cannot change or delete the options of an active or backup configurations.

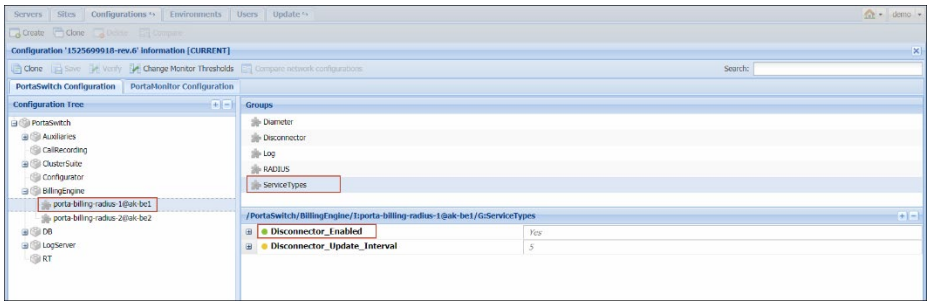
Configuration information

On this page you can see the **Configuration Tree**, **Environments**, **Groups** panels and the panel where all the configuration options for a given service are shown.

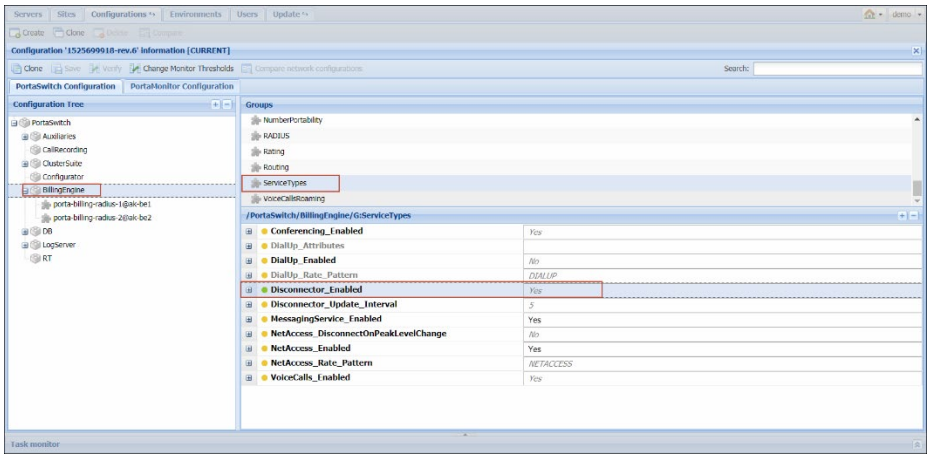


Some options can be specified at the level of the particular instance and at the level of the configuration tree node that holds this instance.

For example, in the **Configuration Tree** panel you can choose **PortaSwitch→BillingEngine→ porta-billing-radius-1@akbilling** and set the **Disconnector_Enabled** option for this instance. (You can find this option in the **ServiceTypes** group.)



But you can also specify the same option at the level of the configuration tree node (**PortaSwitch→BillingEngine→…**).



If you specify the option value at the level of the configuration tree node, it becomes a *default* value for all the instances under this configuration tree node. The Configuration server will choose which value to use according to the following rule:

- If you specify the option value at the level of a particular instance, the Configuration server will use this value and ignore the data specified at the level of the configuration tree node;
- If you leave the option value at the level of a particular instance blank, the Configuration server will use the *default* value – that is, specified at the level of the configuration tree node.

The same rule applies when you specify options for environments.

You can set up configuration options for each billing environment separately or you can do this globally for all billing environments by specifying a *default* value.

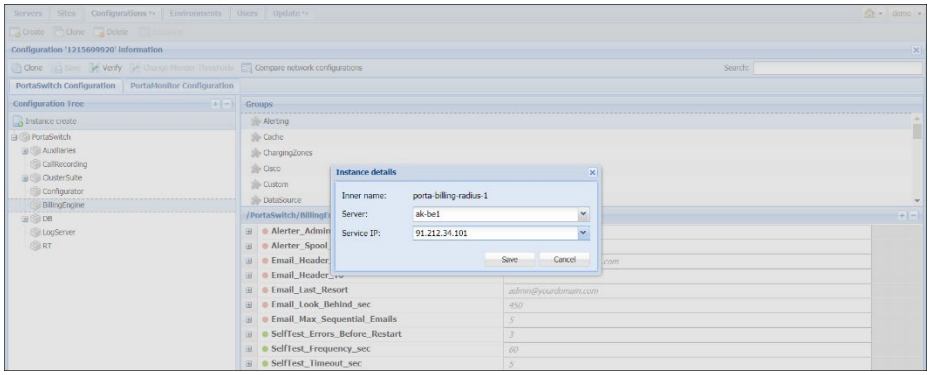
Note that it is not always correct to specify default (global) values for the options since such settings are applied to all instances, some of which may be located on different physical servers. For example, if you set private LADDR (Layered-Architecture Device Driver) for PortaSIP® on the global level, the configuration will be correct as long as all virtual PortaSIP® instances are located on the same physical server. However, if PortaSIP® cluster is deployed within PortaSwitch® installation, there are two or more PortaSIP® servers. In such cases, setting a default value for the private IP address (LADDR) may not be correct since some PortaSIP® instances that are located on other physical servers, may adopt the specified IP address (that doesn't belong to their server).

Instances

A service which runs on your server (e.g. "web interface" or "SIP server") is called an instance. Each service requires its own IP address, so that it can be accessed by your customers. To add a new instance, press the

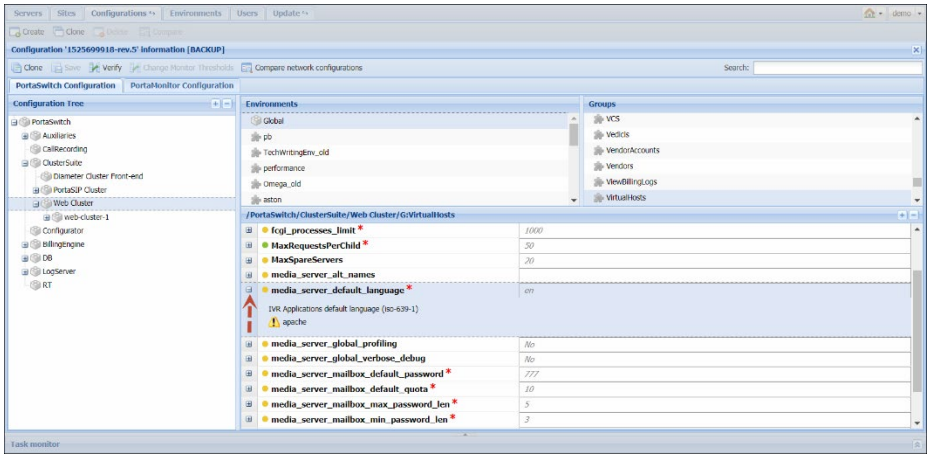
Instance create button. In the pop-up window, choose the server which this instance will run on, its service IP and a billing environment where this instance will run, and then press **Save**.

To change these settings later on select the instance from the configuration tree and double-click on it.



In the configuration options window, you can see instance options with either default values (shown in grey) or explicitly defined values (shown in black). To edit a specific option, double-click on it. You can also add one more value by using the **Add Value** button.

To find additional information about the required option, click the plus sign on the left. Once you open the required option, you will see its description and an alert about possible action in case you change the option value:



If you see red or yellow triangles – the option value change requires a service restart or reload (there might be a period of service downtime when you apply this configuration).

If you want to create one more instance with the same options as in the existing one, use the **Instance clone** button.

After all the values have been set, click the **Verify** button to see the differences between the current configuration and the intended one. Then, click **Check/Apply** button to verify if the configuration is valid (e.g. all the required options have values assigned to them); then on the pop-up window with the status information you can choose whether to perform a complete check or apply the configuration right away.

If you want to check whether any services will be restarted when a new configuration is applied (e.g. for more suitable scheduling) press the **Complete Check** button. The system will simulate the whole procedure and provide a detailed log of actions that will be executed when the configuration is applied.

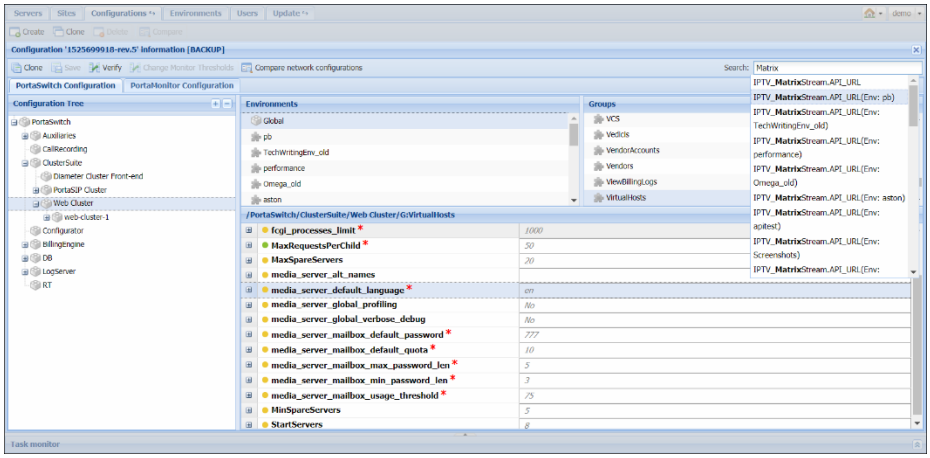
NOTE: When you apply a backup PortaSwitch configuration, the backup network configuration is simultaneously being applied.

If you are satisfied with the results of the preliminary check, press the **Apply** button. As soon as the configuration has been applied, you will see this action displayed on the Task page.

NOTE: The **Check/Apply** button saves the configuration before checking it.

NOTE: We strongly recommend AGAINST applying a configuration that contains instances residing on the servers that in turn are not available (server is down for some reason).

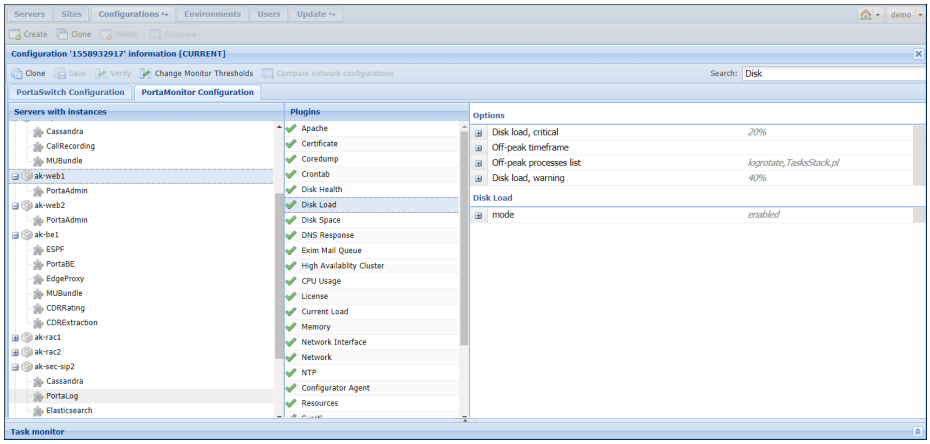
There is also extended **Search** functionality inside each configuration tree that allows you to make a search by the option's name or value, or the name of the instance. Start by simply entering the target value to see all the possible variants.



PortaMonitor configuration

On the PortaMonitor Configuration tab, you can see the list of monitoring plugins enabled in your installation. A monitoring plugin is a script in Perl, Python, Shell or a binary executor, that checks a particular parameter of a server (e.g. Disk health, CPU usage, etc.) or service (e.g. RADIUS cluster, number of MySQL connections, etc.), matches it with the threshold and reports the parameter status to the PortaOne monitoring system. Every minute each parameter is checked.

The monitoring plugins are grouped per server and per instance. To simplify navigation and operation on the PortaMonitor Configuration tab, it is divided into three sections:



The **Servers with instances** section lists all your installation's servers and all the instances running on those servers.

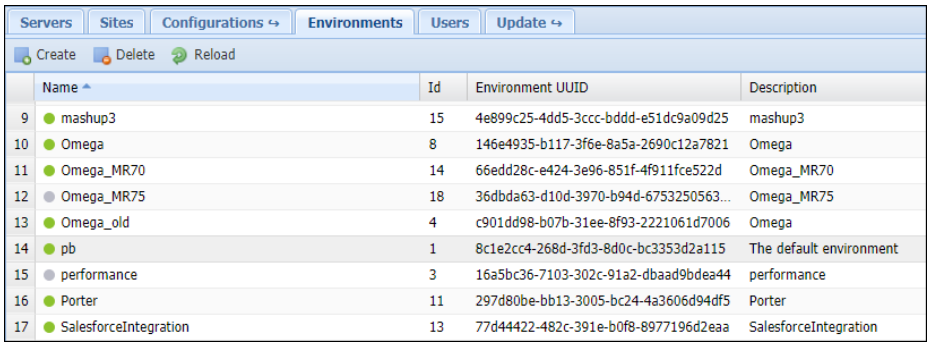
The **Plugins** section lists all monitoring plugins available either on a given server or for a particular instance. The ✔ status icon shows a plugin is enabled; the ✘ icon marks a plugin as disabled and this particular parameter is therefore not monitored. Click the server's name to display its monitoring plugins. Select an instance to view the list of plugins available for it.

Select a plugin and view its configuration thresholds in the **Options** section. Here you can enable or disable the plugin and change its thresholds. Before you make any modifications with the monitoring plugins, we strongly recommend that you discuss them with PortaOne support.

After you have made the changes, click the **Change Monitor Thresholds** button to apply them. To ensure that monitoring thresholds apply to the active server and / or instance, the **Change Monitor Thresholds** button is only active for the currently active configuration.

Environments

On this page you can manage virtual environments.



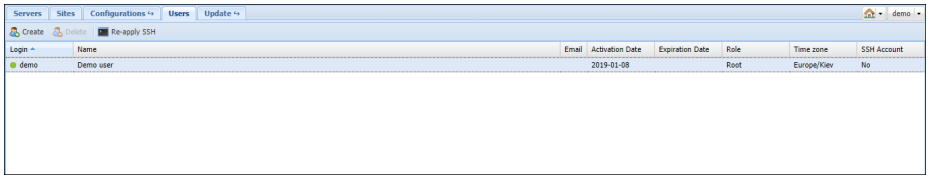
	Name	Id	Environment UUID	Description
9	mashup3	15	4e899c25-4dd5-3ccc-bddd-e51dc9a09d25	mashup3
10	Omega	8	146e4935-b117-3f6e-8a5a-2690c12a7821	Omega
11	Omega_MR70	14	66edd28c-e424-3e96-851f-4f911fce522d	Omega_MR70
12	Omega_MR75	18	36dbda63-d10d-3970-b94d-6753250563...	Omega_MR75
13	Omega_old	4	c901dd98-b07b-31ee-8f93-2221061d7006	Omega
14	pb	1	8c1e2cc4-268d-3fd3-8d0c-bc3353d2a115	The default environment
15	performance	3	16a5bc36-7103-302c-91a2-dbaad9bdea44	performance
16	Porter	11	297d80be-bb13-3005-bc24-4a3606d94df5	Porter
17	SalesforceIntegration	13	77d44422-482c-391e-b0f8-8977196d2eaa	SalesforceIntegration

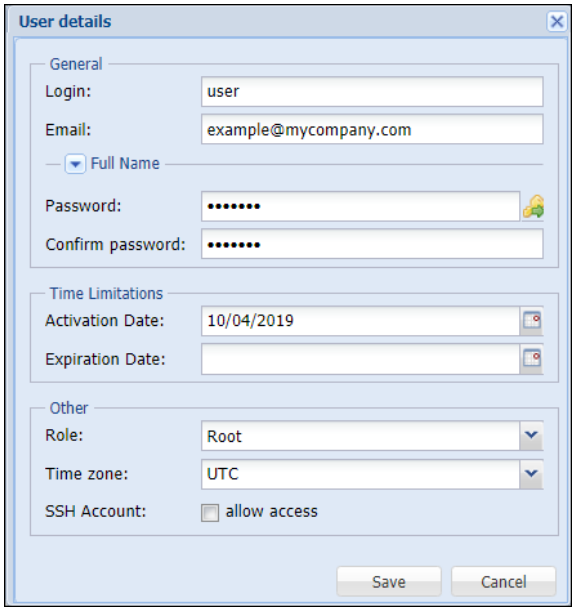
Field	Description
Name	The name of the environment.
ID	The internal ID of the environment.
Environment UUID	The unique ID of the environment. It is not editable and remains intact even if the environment name is changed.
Description	A short description of the environment. This field is not mandatory.

NOTE: Only users with Root and Admin roles can create and delete environments.

Users

This tab is for editing information about users who have access to the Configuration server. To edit, simply double-click on the particular user:





Field	Description
Status	The status of the user: when the button is red, the user is offline; when it is green, the user is online.
Login	Shows which name the user is logged in with.
Email	The email address of the user.
Salutation	Defines which greeting will appear to the user (e.g. Mr., Ms., Mrs., etc.).
First Name	The first name of the user.
Middle	The middle name of the user.
Last Name	The last name of the user.
Password	Allows you to change the password for this user. By clicking the **Auto-generate** icon, a random password is generated.
Confirm password	Repeat the password defined for this user.
Activation Date	The date when the user was activated.
Expiration Date	The date when the user's rights will expire.

Role	Shows the user's role: • **Root** provides access to all options and tabs. • **Admin** provides access to only the **Servers** and **Configurations** tabs. • **Read-only** users have access to all the same tabs as Root but cannot make changes. • **Monitor** only gives access to the monitoring system web interface via the **Monitor** button. • **FileTransfer** users are only used for file upload from remote hosts to the server with the xDR Extraction instance configured.
Time zone	The time zone in which the user is operating.
SSH Account	Indicates whether the user is allowed to log in to servers in the current installation by using SSH.

You can create and delete users using the **Create** and **Delete** buttons, respectively.

NOTE: The user will be able to log in only after the activation date. Likewise, the user will not be able to log in after the expiration date.

The **Re-apply SSH** button allows the creation / recreation of UNIX accounts on all servers for the selected user. This allows the user to log in to servers in the current installation by using SSH, which is required if this user was initially created without SSH access – or if new servers were added to the installation.

Update

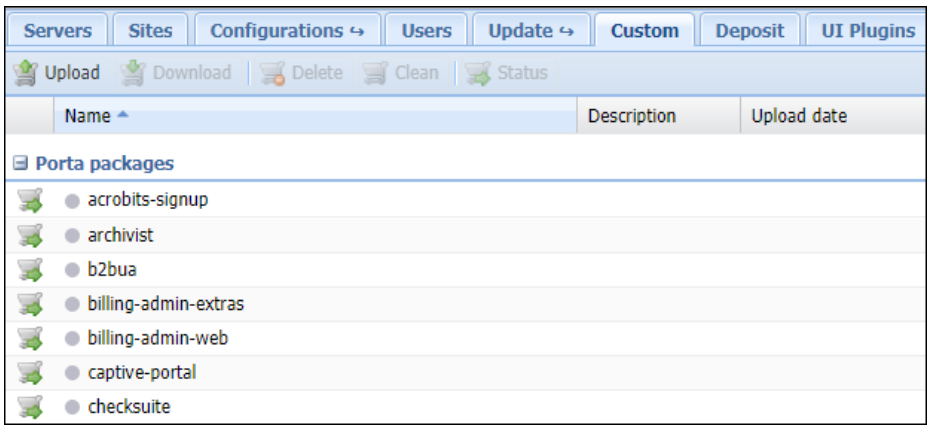
The update is performed via the Configuration server. If you wish to update your system, please contact the PortaOne support team at **support@portaone.com**, who will provide you with further assistance.

Custom

This tab allows you to manage custom software and patches on your servers. When entering this tab you see the list of RPM packages. It is divided into two groups:

- **Porta packages** – list of all PortaOne RPM packages
- **Third-party packages** – already installed third-party RPM packages

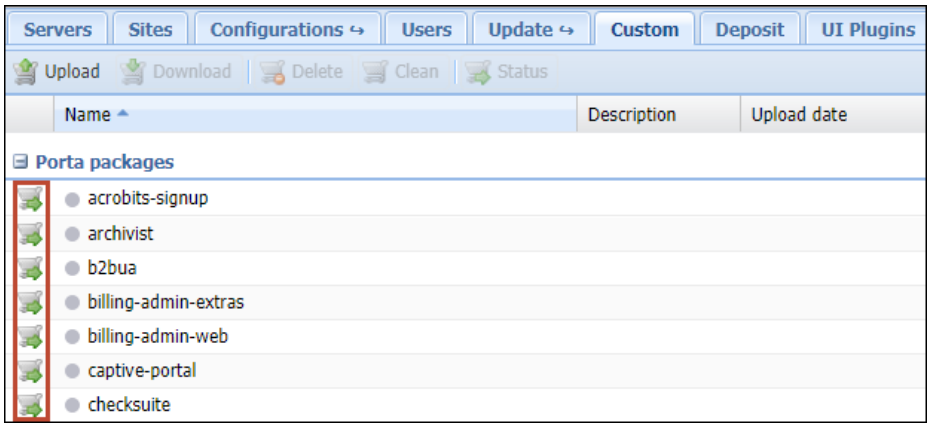
An indicator on the left of the package name shows whether it contains patches (green light), does not contain patches (grey light) or cannot contain patches (red light).



The **Custom** tab provides the following activities:

Field	Description
Upload	Uploads new third-party RPM package.
Download	Downloads third-party RPM package from the server.
Delete	Removes selected RPM package from the repository. This option is only active for third-party RPM packages.
Clean	Removes all patches from the selected RPM package.
Status	Shows status and version of RPM package on all servers within the installation.

If a PortaOne RPM package is patched, its name appears bold in the list. When clicking the icon on the left of the desired package, the **Patches** block opens. This block will contain the list of all patches if they are already uploaded for a particular RPM package.



A patch can have one of three kinds of status:

- **New** (grey indicator) – a patch was uploaded and has or has not been used before
- **Applied** (green indicator) – a patch is currently applied to the RPM package. Click the icon to view logs. Note that patched RPM must be installed to become effective
- **Error** (red indicator) – the application of a patch has failed. Click the icon to view logs

The **Patches** block provides the following activities:

Field	Description
Upload	Uploads a new patch file. You will see a pop-up window where you should choose the file to upload, enter a description and specify a **Lifetime** and **Source code** for a patch.
Download	Downloads a patch from the server.
Build	Rebuilds the selected RPM package with the uploaded patch included. Note that changes won't become effective immediately – the patched RPM must be installed to take effect. For more information see the *Patch upload* section below.
Delete	Removes the patch from the list. **NOTE:** It is prohibited to delete a patch while in an "Applied" state. To remove it, clean the patched RPM package first.
Clean	Removes selected patch from the RPM package or resets error status. Note that changes won't become effective immediately – the patched RPM must be uninstalled for the original RPM to take effect. For more information, see the *Patch upload* section below.

Patch's lifetime

Every uploaded patch has a lifetime parameter. This means the "finish date" for an RPM package or patch propagation.

Why specify a lifetime for a patch

When you modify a PortaOne package, you are actually applying patches on top of an underlying PortaOne code. Since PortaOne developers always work on improving code and adding new functionalities, the software (packages and files they contain) changes with every new release. To make sure that your custom patches are up-to-date after a software upgrade to a new release, you will *always* need to sync your custom patches with the updated underlying code, and fix any hunks in your patches that no longer apply. This is called *rebasing* your custom patches. By setting a

specific lifetime for your custom patches, you ensure that the patch will not be applied to a new release where it hasn't yet been tested by your team. Another example might be when a patch is only applied to certain releases or builds, because in later releases, it loses its viability.

How to use the lifetime of a patch

The lifetime parameter permits the specification of specific software releases and builds. An RPM for a new version with a patch included will automatically be rebuilt and installed (during the PortaSwitch® update procedure).

There can be several patches with different (or the same) lifetimes for one package but only one of them can be active. If there is an active patch (included in a successfully built RPM package) and a new RPM package with another patch has been successfully built, the latter patch becomes active and the former patch becomes "new" (the RPM package with the former patch is removed from the repository).

Lifetime can be one of the following:

- Forever – An RPM package with custom patch included will automatically be rebuilt and installed during every PortaSwitch® update procedure. In case of failure, the PortaOne support team will notify you about the error.
- Release – An RPM package with custom patch included will automatically be rebuilt and installed during a PortaSwitch® update to any build within a specific release.
- Build – An RPM package with custom patch included will automatically be rebuilt and installed during a PortaSwitch® update to a specific build ONLY.

You can specify a Source code for building an RPM package. It can be one of the following:

- Latest – defined by active configuration (e.g. latest hotfix for current build).
- Strict – user defined build string (e.g. "39.0-2.20101213" – source RPM package for MR39-0-1-be).

Note that the above feature is mainly used by the PortaOne support team to manage available hotfixes for a specific RPM package. If you need the list of available build strings, please contact the PortaOne support team at **support@portaone.com**.

In case of a strict build, its string is displayed in brackets in the **Life time** column of the patches list.

Note that for patched PortaOne packages as well as new third-party packages to take effect, they must be installed via a software upgrade (as a separate operation or as part of a PortaSwitch® update procedure). For more information, see the *Patch upload* section below.

Patch application to an RPM package

When you introduce changes, either to PortaOne packages or to third-party ones, you want the changes to remain effective after the software upgrade procedure. To do this it is necessary to prepare a custom patch (a file that describes the differences between the original and modified files) and upload it to the **Custom** tab. Below you will find step-by-step instructions on how to create and apply a custom patch and helpful hints on how to ensure that it works with the new software release.

Note: We encourage you to review your custom patches before the software upgrade to make sure that they can be applied to the updated software in a new release. This is the responsibility of the customer to fix any hunks in the patches that no longer apply.

Patch preparation

To prepare a patch we use a standard "diff" Linux command that makes a line-by-line comparison between the original and modified files and shows the difference in a specific format. Let's consider this example of patching the /home/porta-billing/site_lib/Porta/Modules/VoiceCallsRoaming.pm file if changes were introduced into this module file and the custom modified file was saved as /home/porta-one/VoiceCallsRoaming.pm.patched:

Follow these steps to prepare a patch with your custom modifications. Please note that you will need to run some of these commands with root-level privileges (e.g. use the `sudo` command):

1. Go to the directory where the original file is located:
   ```
   cd /home/porta-billing/site_lib/Porta/Modules
   ```

2. Rename the *original* file to VoiceCallsRoaming.pm.orig, and your *custom modified* file to VoiceCallsRoaming.pm:
   ```
   mv VoiceCallsRoaming.pm /home/porta-one/VoiceCallsRoaming.pm.orig
   mv VoiceCallsRoaming.pm.patched VoiceCallsRoaming.pm
   ```

3. Find the name of the RPM that contains the file. The patch must be applied to this very RPM:
   ```
   rpm -qf VoiceCallsRoaming.pm
   ```

4. The command will have the following output:
   `porta-billing-38.0-3.20131215.el6.noarch`,
   where "`porta-billing`" is the name of the RPM and

`38.0-3.20131215` is the build string

Go to the SRPM (Source RPM) package root folder (See **Appendix B** for the most useful SRPM packages):
`cd /home/porta-billing/`
Now you are in the `/home/porta-billing/` folder

5. Create a patch using this single command:
```
diff -Nau /home/porta-one/VoiceCallsRoaming.pm.orig
site_lib/Porta/Modules/VoiceCallsRoaming.pm >
/var/tmp/VoiceCallsRoaming.pm.patch
```

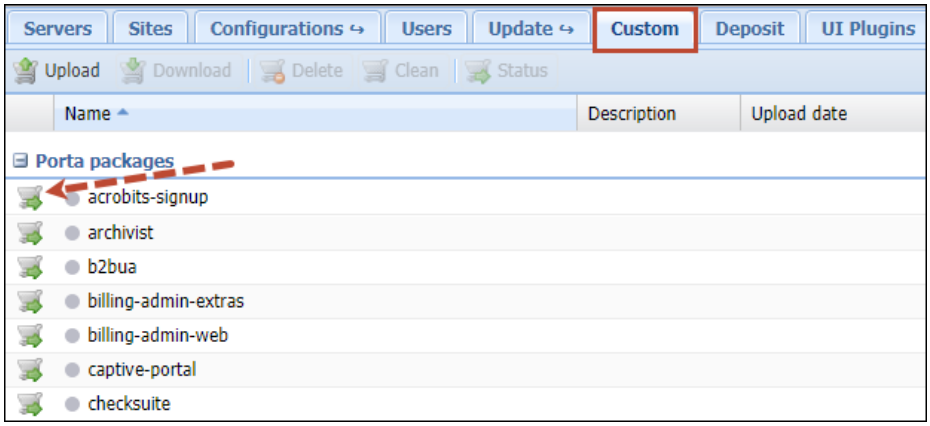
6. Check that the patch was created correctly and that it only contains required modifications:
```
less /var/tmp/VoiceCallsRoaming.pm.patch
```

7. Download this file (`/var/tmp/VoiceCallsRoaming.pm.patch`) to your local PC (if you use Windows OS you may use a program like WinSCP for this)

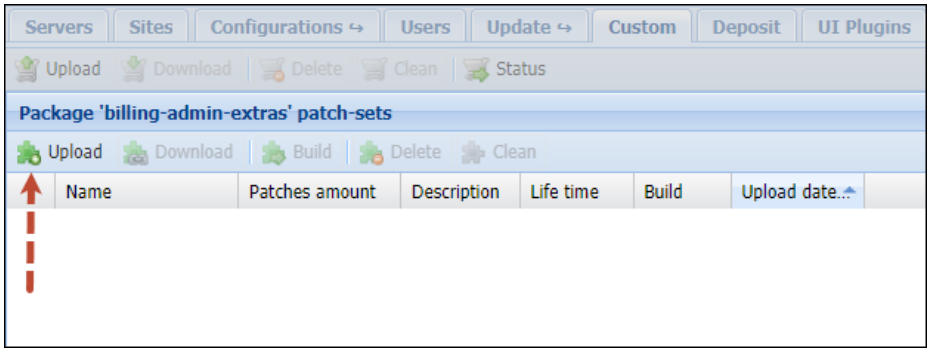
Patch upload

Upload the patch to the **Custom** tab for the 'porta-billing' RPM package and try to rebuild it:

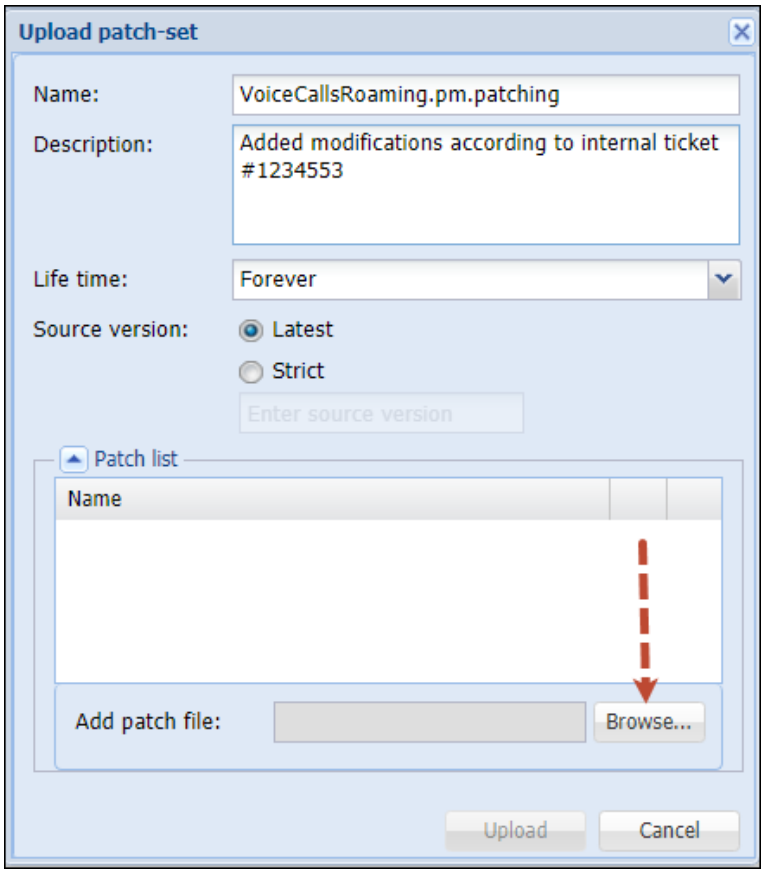
1. Log in to the Configuration server web interface and go to the **Update→Custom** tab. On this tab, select which RPM package to apply the patch to.
2. Click the icon on the left of the desired package to open its **Patches** block.



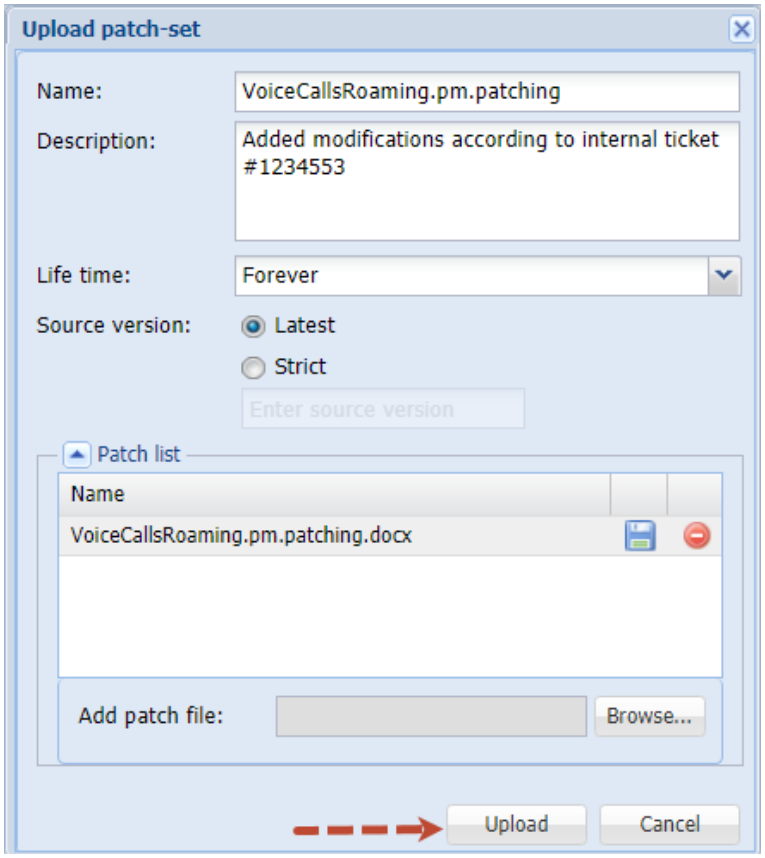
3. Click **Upload**.

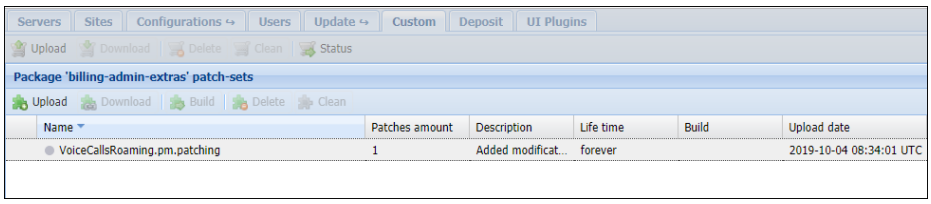


4. Specify the patch name and select the patch file to add it to the list.

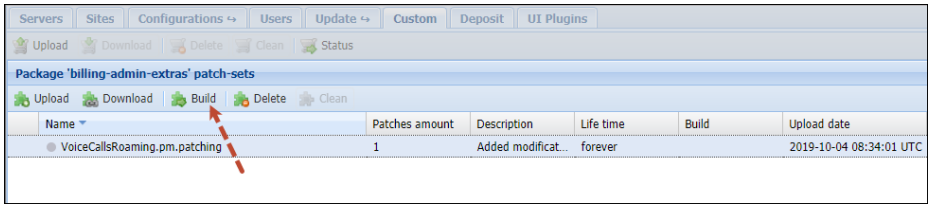


5. When the patch has been added click the **Upload** button.

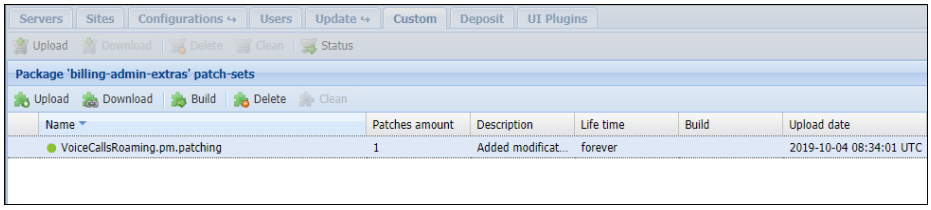




6. Click the **Build** button to rebuild the RPM package with the uploaded patch included.



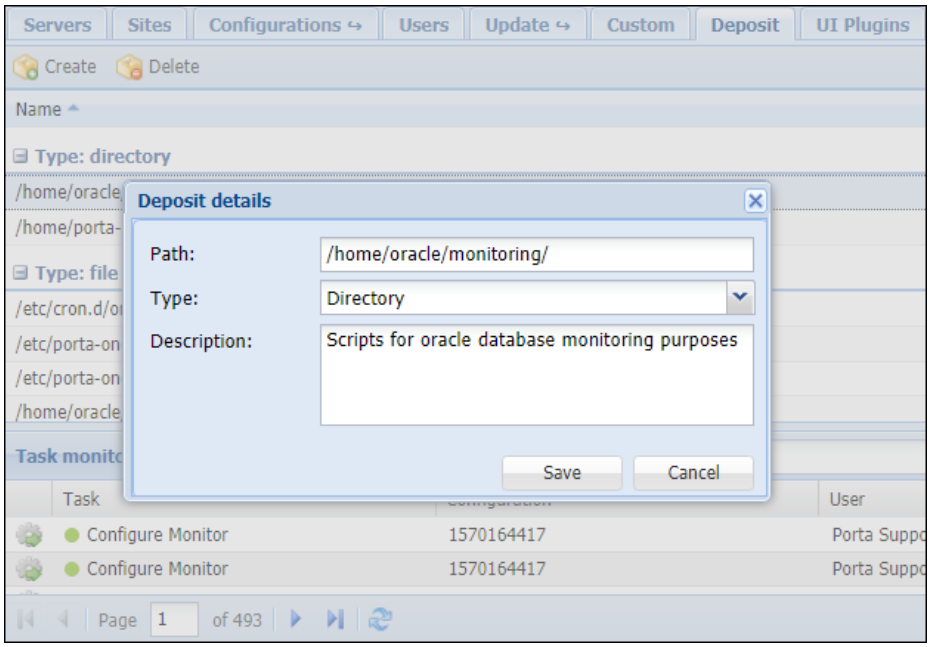
7. If the RPM package with the patch has been rebuilt successfully, you will see the green indicator in the patch **Name** column. If the indicator is red, then the RPM hasn't been rebuilt with this patch and you can click the icon to find the reason in the logs.



8. Now the patched PortaOne package can be installed via the software upgrade (as a separate operation or as part of a PortaSwitch® update procedure). If you wish to install a newly built package, please contact the PortaOne support team at **support@portaone.com**, who will provide you with further assistance.

Deposit

This tab allows you to create a list of custom files (e.g. sudo configuration files) and directories that should remain on your servers during the software upgrade.



When the system is being prepared for a software upgrade to a new release, the files are automatically copied to the partition where the new version of the code is installed, and therefore appear on the production partition after the software upgrade.

Note that files and folders specified on the **Deposit** page *don't* become duplicated; they will be taken directly from specified folders during a software upgrade. Therefore, all changes made to these files after adding them on the **Deposit** page (including removal) will be preserved. For

example, if files are physically deleted from the file system, they will be lost despite the fact that they were added on the **Deposit** page.

UI Plugins

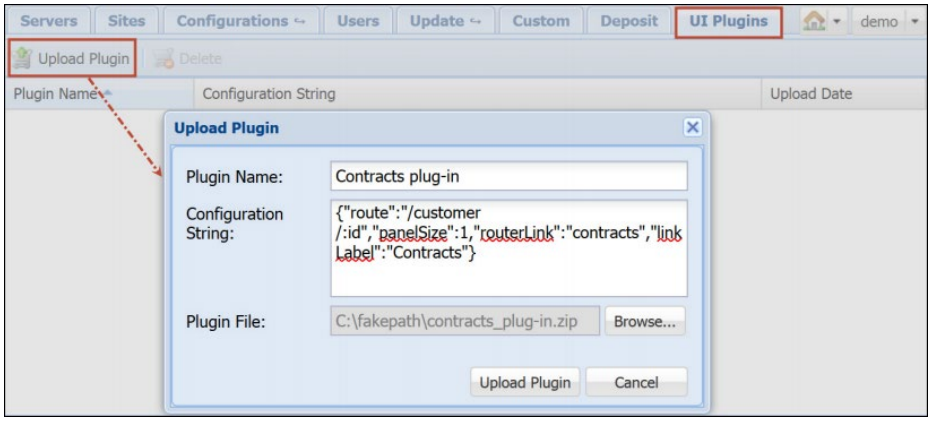
Using plug-ins, you can integrate PortaBilling® with external systems and manage all of the data via the PortaBilling® web interface.

The UI Plugins tab allows you to add plug-ins only once and automatically have them installed on all web servers. Upon adding new web servers, the plug-ins are automatically installed there. They are preserved after a system update to a new release as well.

Plugin upload

Upload the plug-in to the **UI Plugins** tab:

1. Log in to the Configuration server web interface and go to the **Update→ UI Plugins** tab.
2. Click **Upload Plugin**.



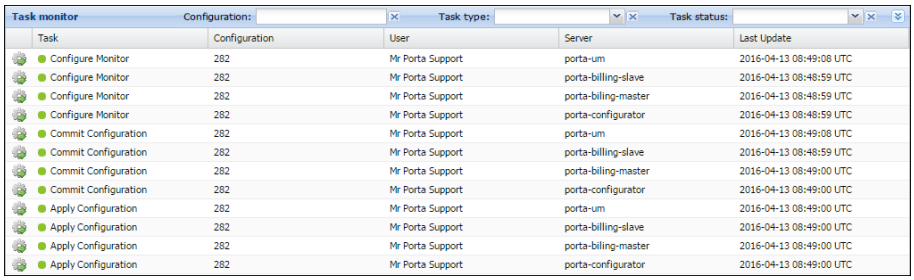
3. Specify the plug-in name and configuration string (JSON string).
4. Select the plug-in file.
5. Click the **Upload Plugin** button.

Task monitor

When you apply a new configuration, the system performs the following tasks:

- Check configuration
- Apply configuration
- Commit configuration
- Configure monitor

Using this tab, you can view information about how configuration changes are applied to the system.



Task monitor Configuration: Task type: Task status:

Task	Configuration	User	Server	Last Update
Configure Monitor	282	Mr Porta Support	porta-um	2016-04-13 08:49:08 UTC
Configure Monitor	282	Mr Porta Support	porta-billing-slave	2016-04-13 08:48:59 UTC
Configure Monitor	282	Mr Porta Support	porta-biling-master	2016-04-13 08:48:59 UTC
Configure Monitor	282	Mr Porta Support	porta-configurator	2016-04-13 08:48:59 UTC
Commit Configuration	282	Mr Porta Support	porta-um	2016-04-13 08:49:08 UTC
Commit Configuration	282	Mr Porta Support	porta-billing-slave	2016-04-13 08:48:59 UTC
Commit Configuration	282	Mr Porta Support	porta-biling-master	2016-04-13 08:49:00 UTC
Commit Configuration	282	Mr Porta Support	porta-configurator	2016-04-13 08:49:00 UTC
Apply Configuration	282	Mr Porta Support	porta-um	2016-04-13 08:49:00 UTC
Apply Configuration	282	Mr Porta Support	porta-billing-slave	2016-04-13 08:49:00 UTC
Apply Configuration	282	Mr Porta Support	porta-biling-master	2016-04-13 08:49:00 UTC
Apply Configuration	282	Mr Porta Support	porta-configurator	2016-04-13 08:49:00 UTC

Field	Description
Configuration search	Filters the tasks based on the configuration name. Administrators can also make a search by internal parameters such as: *i_configuration*, *i_conf*, *apply_id* and *i_server* and their combinations. e.g: i_configuration:1,2,3;i_server:1,2,3; **Note**: use commas to separate several values, use semicolon to separate several parameters
Task type search	Filters the tasks based on the type of the task (e.g. Commit configuration)
Task status search	Filters the tasks based on the success of the task: • **failed** – tasks that have not been completed due to errors • **succeeded** – tasks that have been completed successfully • **running** – tasks that are in progress • **new** – tasks that will start later
The icon	The log for configuration changes. Click the icon to see the log.
State indicator	Indicates the state of the task: • **grey** indicates that the task has started. • **blinking green** indicates that the task is in progress. • **green** indicates that the task has been completed successfully. • **red** indicates that an error has appeared. Check logs to obtain additional information.
Task	Shows the action to be performed to apply a new configuration.
Configuration	Shows the name of the configuration that is applied.
User	Shows who applies the configuration.
Server	Shows the server where the task is performed.
Last Update	Shows the time when the tasks have been performed.

At the bottom of the page, below the **Task monitor**, you can see the page related options. You can go to the next page or the previous one, jump to the first or last page, or use the **Refresh** button to update any of the pages.

3. Initial configuration of PortaSwitch®

Once you have installed the software on the servers, you have a blank system which can be configured in various ways to meet your business requirements. The Configuration server allows you to specify a role or even a set of roles to be assigned to each server. This chapter will demonstrate how to set up the initial configuration of the system.

Checklist

Print the following page and perform the system setup by following the instructions, using them to check off the operations you complete. Please be sure to perform all of the operations (all of the boxes should be checked); otherwise the system will not work as desired.

Operation	Done
Add servers	[ ]
Create configuration	[ ]
** Add main instances*	[ ]
Add three Cassandra instances	[ ]
Add MasterDB instance	[ ]
Apply the configuration	[ ]
Add StandByDB instance (optional)	[ ]
Apply the configuration	[ ]
Add ReplicaDB instance	[ ]
Apply the configuration	[ ]
Add BillingEngine instance	[ ]
Add web cluster instance	[ ]
**** Add a SIP cluster and define its virtual IP address	[ ]
***** Add two DispatchingNode instances	[ ]
Add two ProcessingNode instances	[ ]
Add VoiceMailDB instance	[ ]
Add Elasticsearch instance	[ ]
Add LogServer instance	[ ]
Add additional instances (optional)	
Add RTDB instance	[ ]
Add RT instance	[ ]
Add CallRecording instance	[ ]
Create Auxiliaries such as SMSTrigger, STUN Server and / or XDRImport	[ ]
Apply the configuration	[ ]
Create new billing environments as needed	[ ]

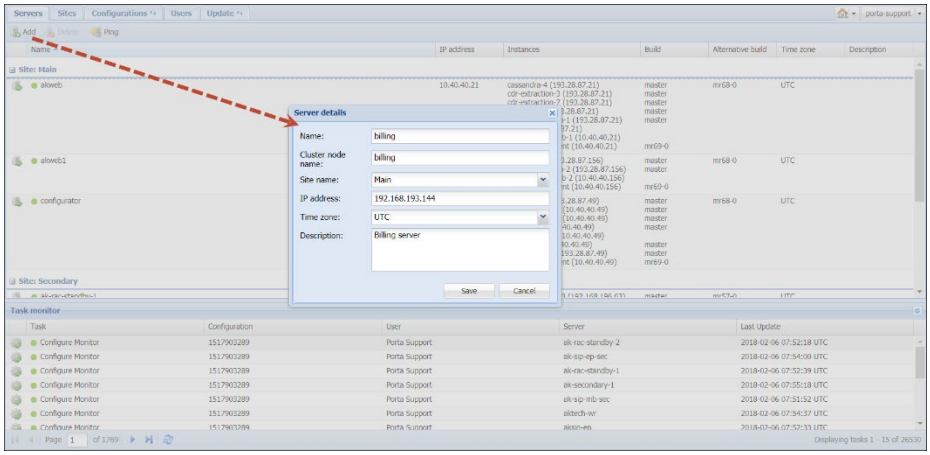
*** Adding the main instances should be performed in the foregoing order.
**** Virtual IP address can only be an address that is not assigned to any instance or server as the service IP.
***** DispatchingNode instances must each be added on their own physical servers.

We recommend that you follow all the above steps in the suggested order in order to avoid issues during configuration. Some components may have external prerequisites that must be satisfied in order to be configured properly. For instance, to correctly set up database replication, the **MasterDB** must be configured before the **ReplicaDB**.

Add servers

Adding servers is the first step of your initial system configuration (depending on your specific type of installation, the number of servers can vary).

1. Go to the **Servers** tab.
2. Click the **Add** button on the toolbar, and fill in the fields in the **Server details** dialog box:



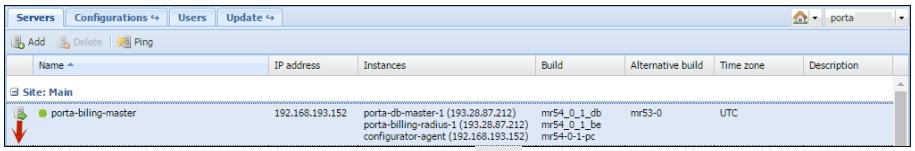
NOTE: When adding a server to the installation on this page an IP is specified. This IP is automatically considered internal so it and its NIC become read-only in Network configuration UI.

3. Click **Save**.

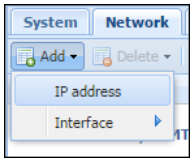
Add IP addresses

Once you have added servers, you can add public IP addresses that will be assigned to the particular instances in the later steps of the PortaSwitch® configuration.

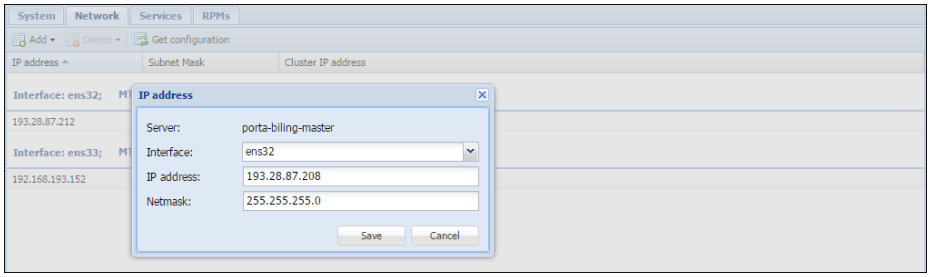
1. On the **Servers** tab, choose the server for which you wish to add a public IP address, and click **Change server configuration**.



2. Go to the **Network** tab, click **Add**, and choose **IP address**.



3. In the **IP address** dialog box, specify the following information:
   - **Interface** – You can select only public interface here
   - **IP address**
   - **Netmask**



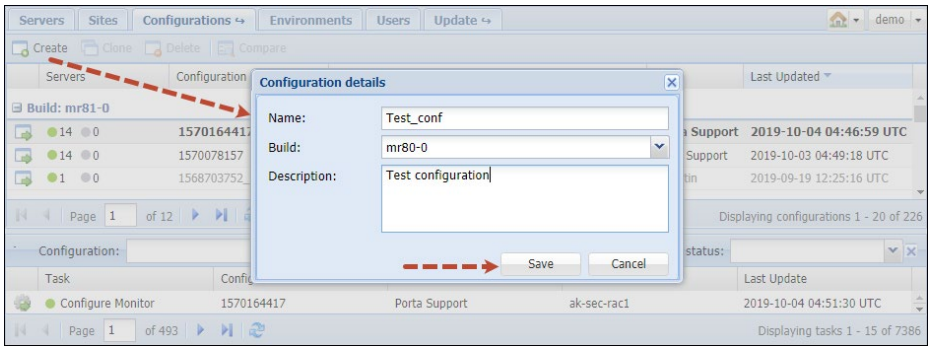
4. Click **Save**.

In case you want to run several service instances on one physical server, you need to first associate the additional IP addresses with the public network interface of the server (this process is called "IP aliasing"). To do this, repeat steps 1–4, and specify the required IP alias in step 3.

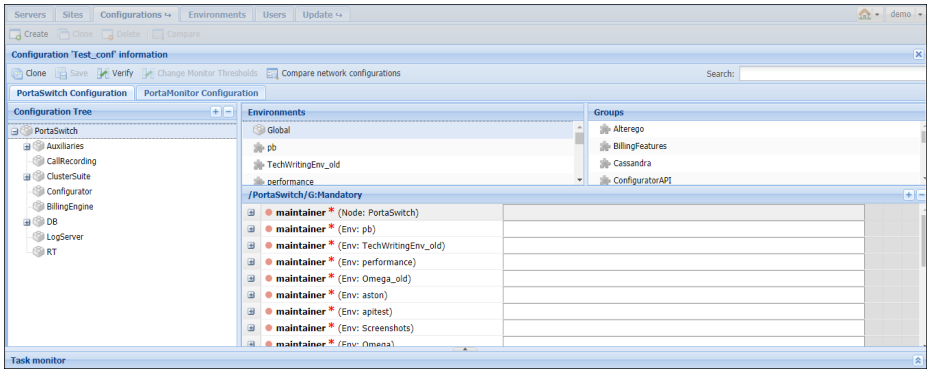
Create a configuration

After you have added all the required servers, go to the **Configurations** tab. Here you can create a configuration to fit your needs.

To create one, press the **Create** button and then specify its name and description and choose which software version it applies to.



You will see a Configuration Tree, Environments, Groups panels, and the panel where all the information about a given service is shown.



Add instances

Interaction specifics

When adding instances, keep in mind the following idiosyncrasies of their interaction:

- If there are two or more instances that depend on the Apache web server (at the moment these are: **Web**, **SMSTrigger**, **RT**), they must be configured with different IP addresses ('service IP') or ports. Otherwise, the Configuration server will display warnings during the configuration check and the configuration will not be applied.

- In order to keep the system working efficiently, do *not,* under any circumstances, put the following instances on the same server:
  - MasterDB and ReplicaDB
  - BillingEngine and LogServer

Instances necessary for a secondary site

Note that for a secondary site to provide all the necessary services in standalone mode, the following minimum set of instances must be configured on it:

- **BillingEngine** – This instance calculates applicable charges according to product, tariff and other billing parameters.
- PortaSIP® Cluster instances: one **Dispatching Node** and one **Processing Node** – Each of these instances is necessary for voice termination, transmission of instant messages and Media Server functionality. These instances are not required if you do not provide any of these services (for example, if you exclusively provide Internet access).

- **OracleDB** or **StandByDB** (depending on what type of database you use, Oracle or MySQL) – StandByDB is an actual replica of the MasterDB, and as such, provides all the information about existing accounts, products, service configuration, etc. when the MasterDB is unavailable. Note that new xDRs are stored in a special database with deltas. You do not need to add those instances independently. When the primary site becomes available again, information from the database with deltas is synchronized into the MasterDB.

  For Oracle the procedure is similar, but in this case a database administrator manually defines which OracleDB instance will be for the "master" database, which one for "standby" and which one for the "database with deltas."
- **Web Cluster** – While the web interface is not available in standalone mode, this instance also runs Apache services that are responsible for the callback feature and several other IVRs, and also XML / JSON API access. Configure this instance if you require such functionality in standalone mode..
- **LogServer** – This instance is responsible for storing BE logs and together with Elasticsearch, for storing SIP logs.
- **Elasticsearch** with the **with_indices** option set to **logs** – Together with LogServer this instance is responsible for storing SIP logs.

Note that Media Server functionality and XML / JSON API access are limited in standalone mode. For more information, please refer to the **PortaSIP Media Applications Guide**, **PortaSIP XML / JSON API Reference Guide** and **PortaBilling XML / JSON API Reference**.

Auxiliary functionality, such as Call Recording, xDR Mediation or Request Tracker system access is unavailable in standalone mode.

How to add all necessary instances

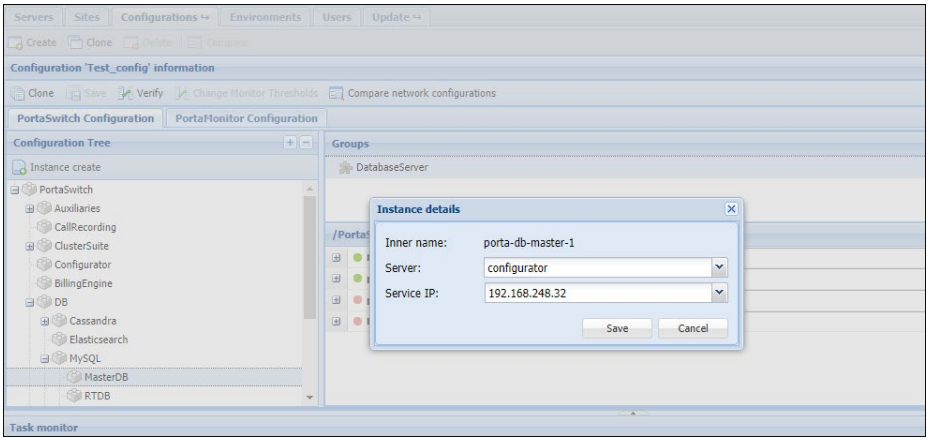
Perform the following steps (using the checklist above to maintain order):

1. From the Configuration Tree, choose DB→Cassandra.

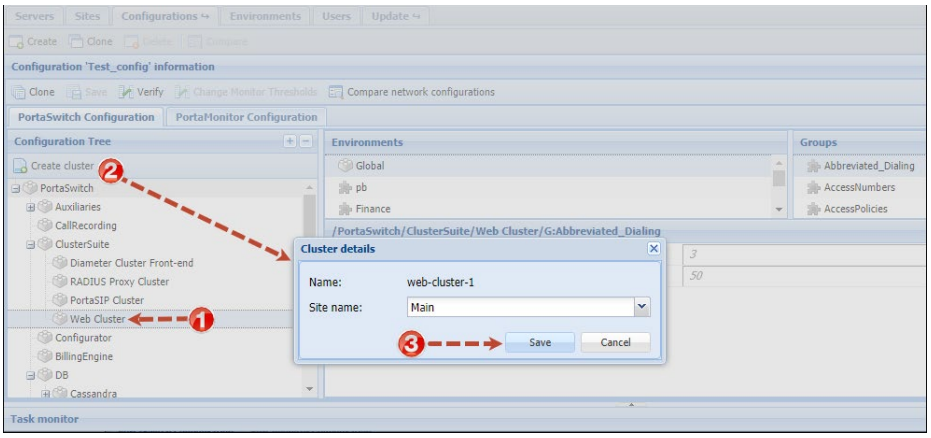
   NOTE: Three Cassandra instances must be added in all. These instances can be created on servers that do not have databases (e.g. Configurator, Admin, PortaSIP®, etc.). We suggest that you place these instances on servers that have large amounts of RAM and choose internal IP addresses for each of the three Cassandra instances.

2. Click the **Instance create** button. In the **Instance details** dialog box, choose which server this instance will run on and its service IP, then click **Save**.

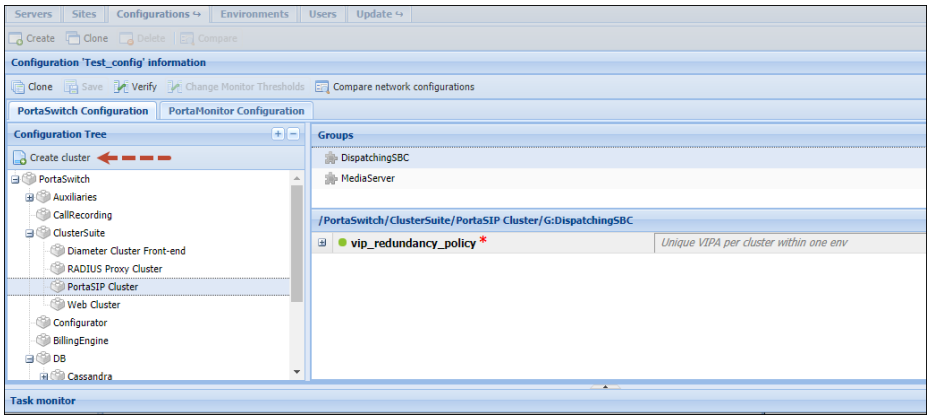
3. Repeat steps 1–2 to add two more Cassandra instances on two other servers.
4. From the Configuration Tree, choose DB→MySQL→MasterDB.
5. Click the **Instance create** button. In the **Instance details** dialog box, choose which server this instance will run on and its service IP, then click **Save**.



6. Specify all required options.
7. Click **Save**, and then click the **Verify** button.
8. Verify the new configuration and click the **Check / Apply** button to see whether the configuration is valid (e.g. all the required options have values assigned to them). Next, click the **Apply** button. As soon as the configuration is applied, you will see this action displayed at the bottom of the **Task** page.
9. Clone the applied configuration. To do this, click the **Clone** button on the **Toolbar**.
10. From the Configuration Tree, choose DB→MySQL→ReplicaDB, and click the **Instance create** button. Fill in the fields in the **Instance details** dialog box and click **Save**.
11. Repeat steps 7–8 to finish the process of adding the ReplicaDB instance.
12. From the Configuration Tree, choose BillingEngine. Add the BillingEngine instance as described in steps 5 and 6.

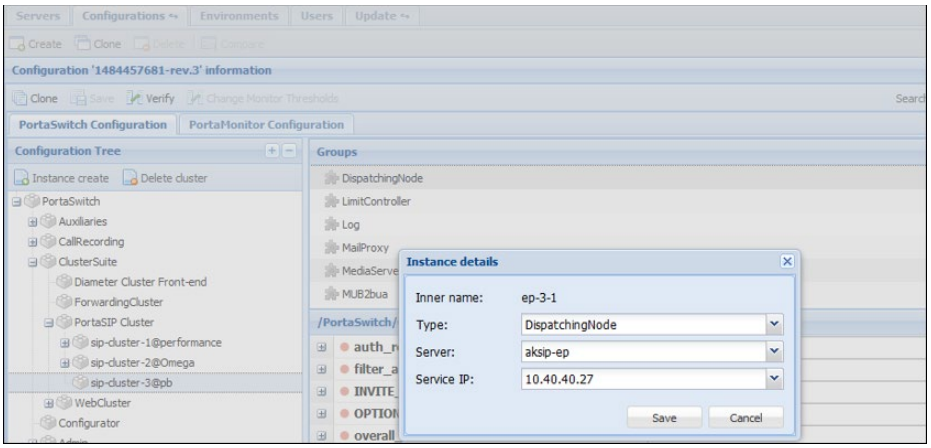


13. From the Configuration Tree, choose ClusterSuite→Web Cluster and then click the **Create cluster** button. In the **Cluster details** dialog box, select which site the web cluster will be configured for. Click **Save**.
14. Click the **Instance create** button. Select the server this instance will run on and its service IP. Click **Save** to save the instance.

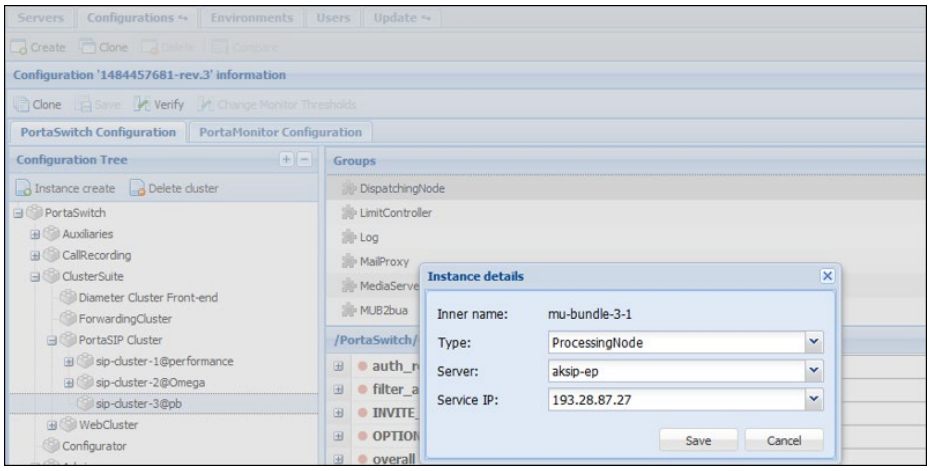


15. From the Configuration Tree choose ClusterSuite→PortaSIP Cluster and then click the **Create cluster** button. In the **Cluster details** dialog box, select the site and the environment the PortaSIP® cluster will be configured for. Click **Save**.
16. Choose the newly created sip cluster and specify its virtual IP address in the **vipaddr** field of the **DispatchingNode** group.
17. Specify the cluster domain name in the **sip_domains** field of the **DispatchingNode** group. The domain name must resolve on the virtual IP address. To add another domain name, click the icon.
18. Specify the domain names for callback and voicemail services in the **callback_domain** and **email_domain** fields of the **Media Server** group. We recommend that callback and email domain names resolve on the virtual IP address.

19. Click the **Instance create** button. Select the **DispatchingNode** instance type, then select which server this instance will run on and its service IP. Click **Save** to save the instance.



20. Add another DispatchingNode instance by repeating step 17.
21. Choose the desired sip cluster and click the **Instance create** button. Select the **ProcessingNode** instance type, then select which server this instance will run on and its service IP. Click **Save** to save the instance.

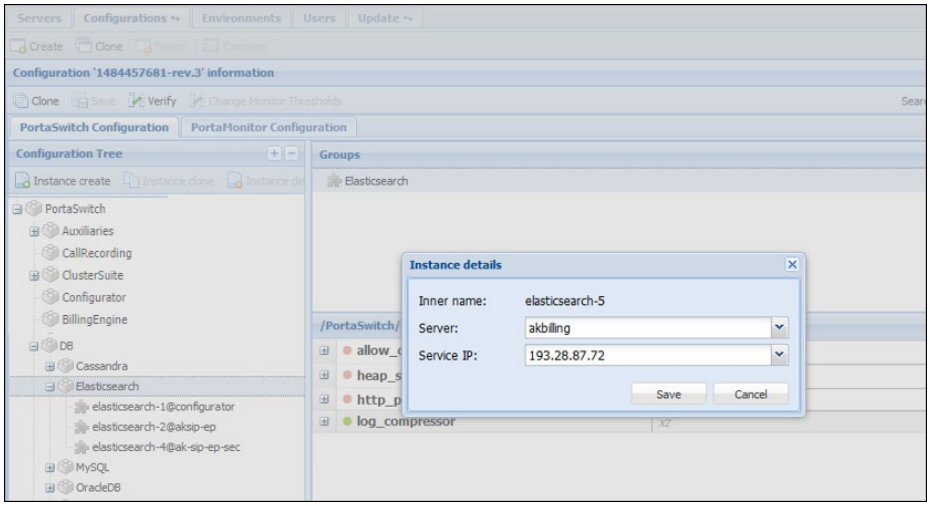


22. Repeat steps 19 to add the desired number of ProcessingNode instances.

NOTE: It is possible to add both a DispatchingNode and a ProcessingNode instance on the same physical server.

23. From the Configuration Tree choose **DB→Elasticsearch** and then click the **Instance create** button. In the **Instance details** dialog box, choose which server this instance will run on and its **service IP**, then click **Save**. Configure the **heap_size** for the Elasticsearch instance depending on the available RAM. The

recommended heap size value is in the range of 25% to 50% of RAM.



24. Add the LogServer and VoiceMailDB instances just as you did for the previous ones.
25. Add other instances by repeating steps 5–6.

NOTE: While adding additional instances to the configuration make sure that you have specified additional IP addresses on the server's **Network** tab.

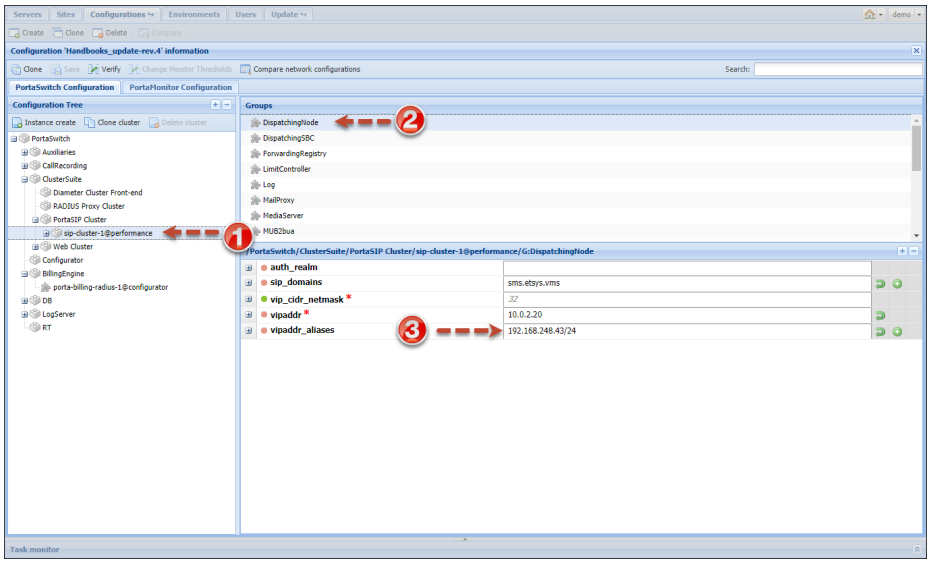
26. Make sure you apply the configuration after all the required instances are added and their options set.

4. How to ...

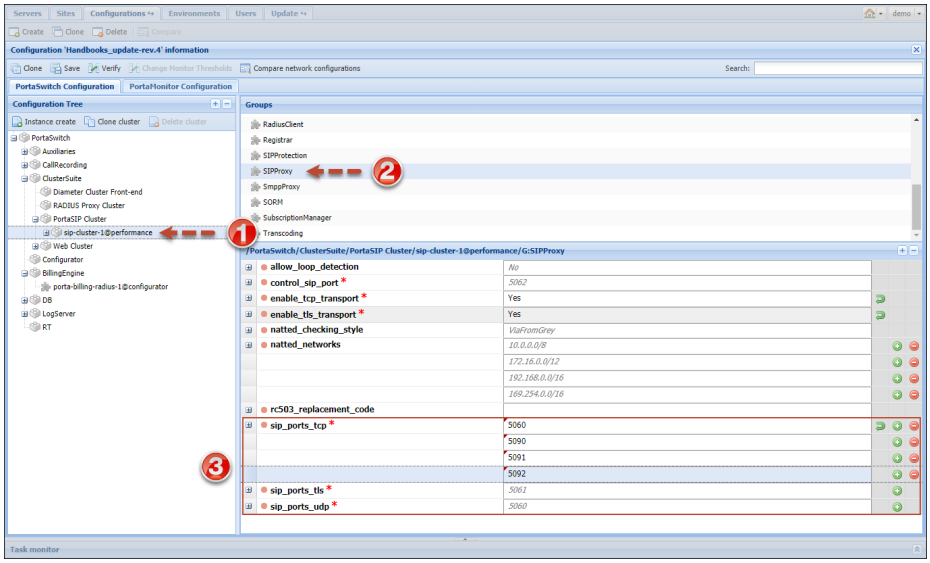
… Add an alias to the PortaSIP® cluster's IP address

An administrator can assign multiple IP addresses as entry points into the cluster (also known as IP aliases). All of these IPs are shared between dispatching nodes of the cluster in the high-availability mode. This allows seamless migration to PortaSwitch® customers with pre-configured IP phones in case of acquisition. Also using alternative IPs and ports as entry points may help to deliver the service in the countries where standard VoIP may be blocked.

1. Open the **Configurations** tab.
2. Clone the existing configuration by clicking the **Clone** icon.
3. In the **Configuration Tree** of the cloned configuration, select **sip-cluster node**.
4. In the **Groups** panel, select **DispatchingNode**.



5. Select the **vipaddr_aliases** option and type a PortaSIP® cluster's IP alias using the following format: `IP address/CIDR`.
6. Select **SIPProxy** group.



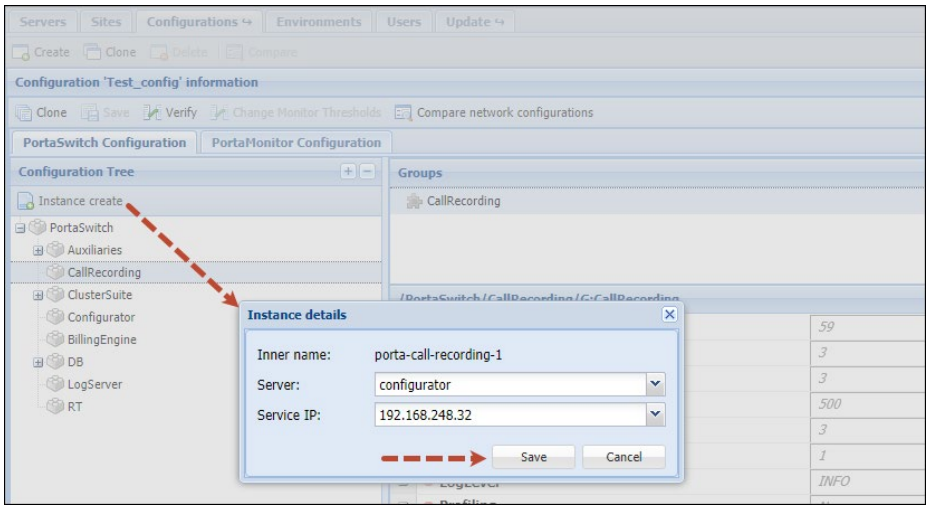
7. Define additional transport ports for the following protocols: UDP, TCP and TLS. This step is optional and only required if standard transport ports for these protocols are blocked for some reason or cannot be used:
    - Select the **sip_ports_tcp** option and click the **Add value** icon. Type an additional TCP port.
    - Select the **sip_ports_tls** option and click the **Add value** icon. Type an additional TLS port. (The default value is **5061**).
    - Select the **sip_ports_udp** option and click the **Add value** icon. Type an additional UDP port. (The default value is **5060**).

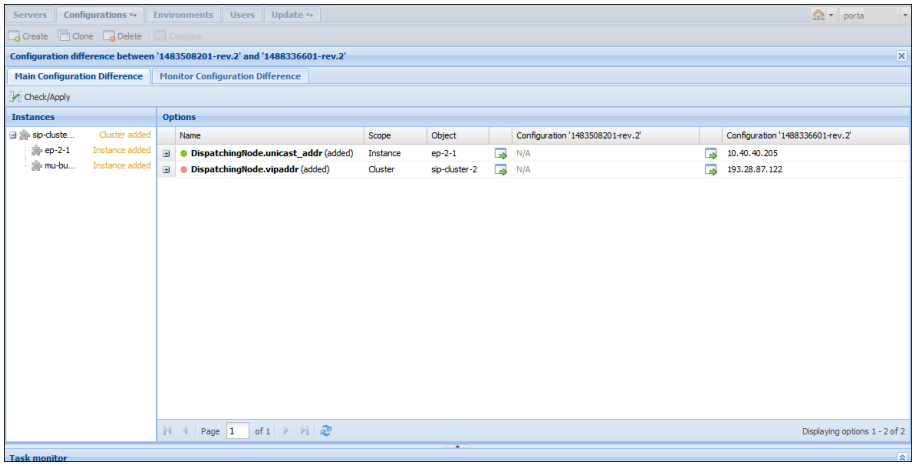
8. After all the changes have been made, click the **Verify** button.
9. Verify the new configuration and click the **Check / Apply** button.

... Change configuration options?

At times you may need to change the options within an existing configuration. For instance, you want to have the ability to record phone conversations for an IP Centrex user and to play back the records later. In order to enable the required functions you will need to change your configuration options. This can be done as follows:

1. Go to the **Configurations** tab.
2. Clone the existing configuration by pressing the **Clone** button.
3. In the **Configuration Tree** of the cloned configuration, choose the **CallRecording** node.
4. Click the **Instance Create** button.
5. In the **Instance details** dialog box, select the server on which this instance will run and the service IP, and then click **Save.**
6. Select the newly created CallRecording instance.
7. Define options for the CallRecording instance (CleanUpPeriod, LogLevel, etc.).
8. After all the changes have been made, click the **Verify** button.
9. Verify the new configuration and click the **Check / Apply** button.





… Configure a MySQL database white list

To add a new IP address to the MySQL database instance white list, follow these steps:

1. In the **Configuration Tree** panel, choose **DB→MySQL→** *Database Instance Type →Database Instance* (e.g. DB→MySQL→MasterDB→*instance@server*).
2. Under the **allow_connection_from** option, specify the IP addresses you want to add to the white list.

   You can specify as many IP addresses as needed. To do this, add either a single IP address or a block of IP addresses in the CIDR notation format – X.X.X.X/Y (e.g. 192.168.99.0/24).

   Note that all server / service IPs of the **PortaSwitch®** installation are already allowed by default.

Each of your MySQL databases can have its own white list.

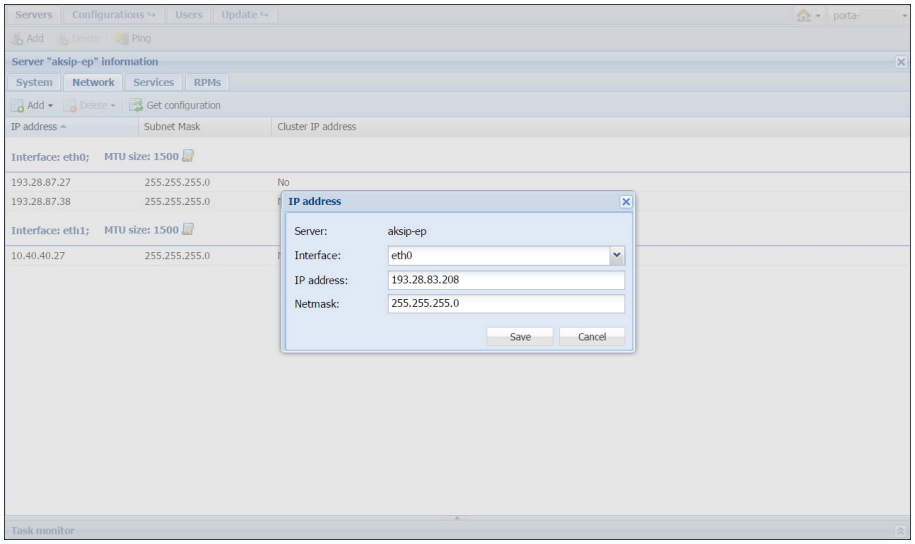
... Configure several PortaSIP® clusters in PortaSwitch®?

PortaSwitch® can be partitioned in multiple virtual environments. Each virtual environment will have its own PortaSIP® cluster with a single entry point (the virtual IP address) running on the existing set of servers.

To configure a PortaSIP® cluster on the existing server, you first need to *associate the additional* IP addresses with the public network interface of the server (this process is called "IP aliasing"). Then you can create the cluster instances on said server, assign an individual IP address and associate the billing environment to each of them. It is recommended that on all servers within the set, you add the DispatchingNode instance (it is on standby) for redundancy and the ProcessingNode instance for load distribution.

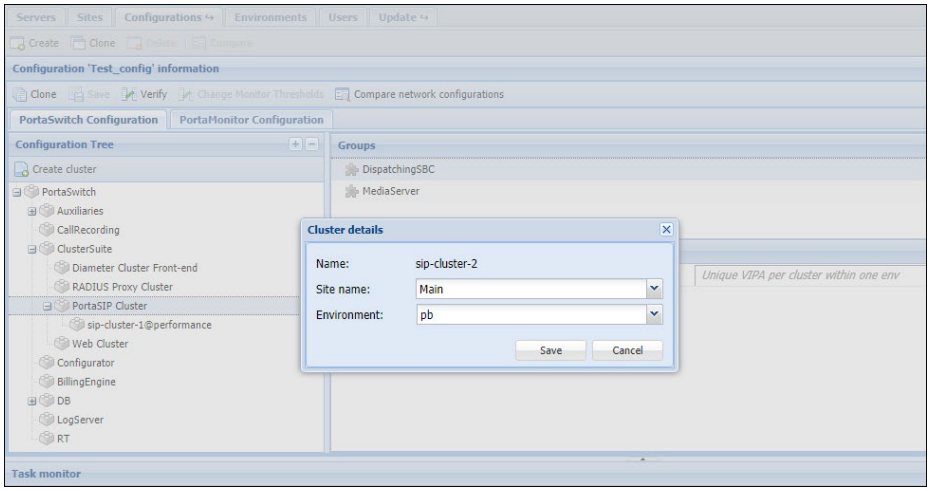
To deploy a new PortaSIP® cluster, complete the following steps:

1. On the **Servers** page, select the server where you want to run the cluster DispatchingNode and ProcessingNode instances.
2. Go to the server's **Network** tab and add the appropriate IP address as an alias.

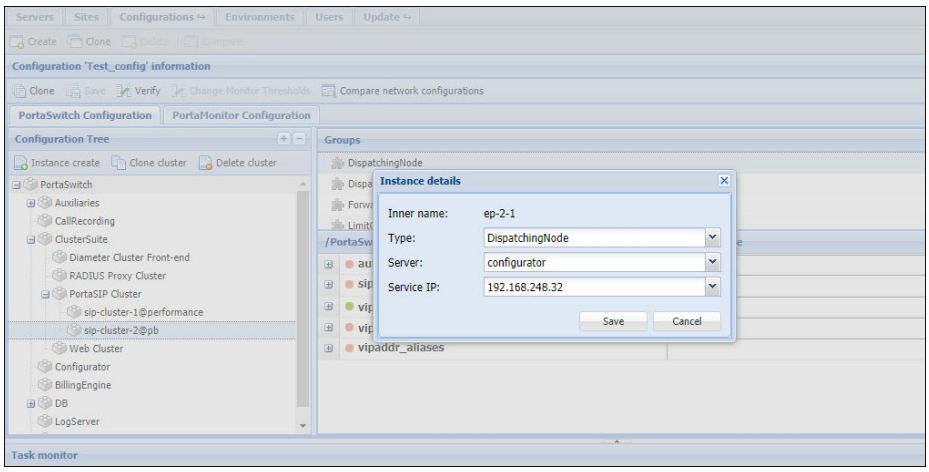


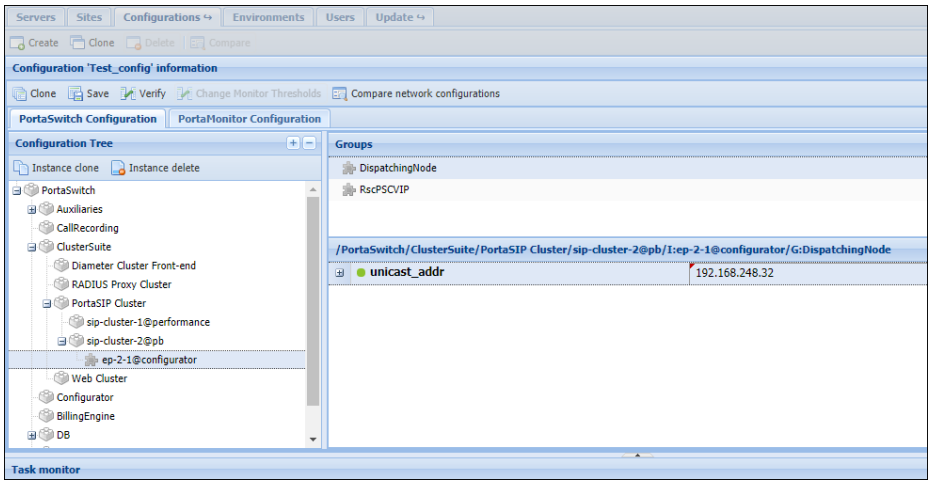
3. Repeat step 2 to add the required number of IP addresses.
4. Repeat steps 1–3 to add IP addresses to another server of your PortaSIP® cluster.
5. Clone the configuration.

6. In the **Configuration Tree** panel, go to ClusterSuite→PortaSIPCluster→Create cluster and press the **Create cluster** button.
7. In the **Site name** field select the site and in the **Environment** field, specify the billing environment where this instance will run. Then click **Save**.

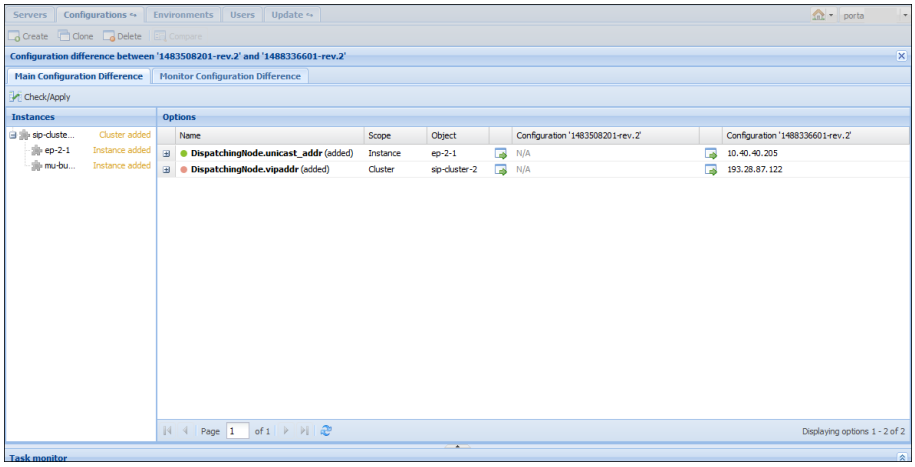


8. Specify the virtual IP address for this sip cluster in the **vipaddr** field of the **DispatchingNode** group.
9. Specify the domain names for callback and voicemail services in the **callback_domain** and **email_domain** fields of the **Media Server** group. It is recommended that callback and email domain names resolve on the virtual IP address.
10. Click the **Instance create** button to create a new dispatching node instance. In the **Type** field select **DispatchingNode**. Then, specify the billing environment where this instance will run and the newly added IP address in the **Instance details** dialog window, then click **Save**.





11. Create a processing node instance. Click the **Instance create** button. Select the **ProcessingNode** instance type, then select which server this instance will run on and its service IP. Click **Save** to save the instance.
12. Repeat steps 6–11 to add DispatchingNode and ProcessingNode instances for another server within your PortaSIP® cluster.
13. After all these changes have been made, click **Save** and then **Verify**.



14. Click **Check / Apply** to apply the configuration.
    Create a new PortaSIP® node via the PortaBilling® admin interface.

… Configure an adaptec RAID health monitoring?

PortaOne monitoring system can collect and analyze disk health information for an Adaptec RAID. This will help you be sure that your hard drives are capable of safely storing your data.

Due to licensing specifics, it is necessary to download and install the corresponding package manually. To do this, perform the following:

1. Download the Adaptec ARCCONF Command Line Utility from **www.adaptec.com**. You can use the following link:

   www.adaptec.com/en-us/speed/raid/storage_manager/arcconf_v2_00_21811_zip.php

2. Unzip the arcconf binary file from the downloaded archive.
3. Copy it to the /usr/bin/ directory on the server that uses Adaptec RAID.
4. Go to the **Deposit** tab on the Configuration server web interface (**Update** -> **Deposit**) and create the following deposit there:
   - **Path** – /usr/bin/arcconf
   - **Type** – File

It is recommended that you not install the full RMP provided by Adaptec as it contains redundant files.

If you are using Adaptec RAID and the package is not installed, you will see the corresponding warning message on the Monitor.

… Configure a backup procedure?

For how to configure a backup procedure please refer to the **Configure Backups with Archivist** handbook of the **Unified PortaSwitch Handbook Collection**.

… Create new billing environments?

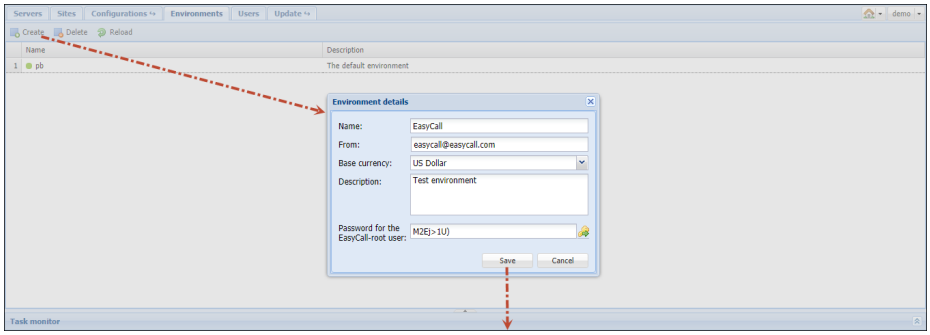
By default, PortaBilling® already contains one billing environment called "pb." This environment is created automatically during the installation of the system. However, you can create additional BE-environments if needed.

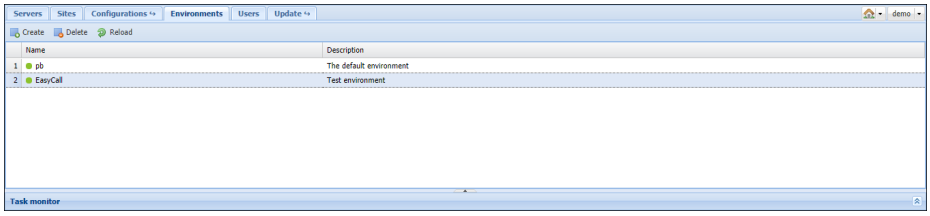
In order to create a new environment:

1. Go to the **Environments** tab, and click the **Create** button.
2. In the **Environment details** dialog box, enter the name, your email address for outgoing communication, base currency and description of the future environment.

   NOTE: You define the base currency only once and cannot change it once you save the environment. The default base currency is US dollars.

3. Copy the generated password or click  to generate another password and copy it there.
4. Click **Save**.





A new environment is created empty except for a single user account that you use to log in and then create other users, tariffs, customers, etc.

By default, the account's username is <env>-root, where <env> is the name of the environment you just created. So, if you create the environment EasyCall, to log into it you use the username EasyCall-root.

For security reasons the user's password is randomly generated and it is displayed only during the environment creation step. Thus, you must copy the password before you click the **Save** button. You will be notified to change this password right after you log in to the admin interface for the first time.

... Configure site-to-site VPN tunnels for PortaSwitch®?

To ensure secure communications between sites within your installation and their proper management by the Configuration server, the servers of these sites must be organized into a single virtual private network. PortaSwitch® provides a built-in VPN solution to do just that.

A site-to-site VPN uses tunnels to create data packets from ordinary IP packets and then to forward them to the remote server over a public network. Encryption is used to ensure their security.

To build a VPN tunnel between the sites means to configure a VPN endpoint on every site and enable connectivity between them.

The sections below describe how to configure VPN endpoints for sites deployed on the premises and hidden behind NAT.

General requirements

1. VPN endpoints must be reachable over a public network. Thus, they must have a public IP address assigned to them.
2. If sites are hidden behind NAT, a VPN endpoint can be configured on private IP addresses, since it is NAT that serves as the communication point.
3. The internal IP address of a VPN endpoint must belong to the same subnet as the internal IP addresses of the servers of the same site.
4. VPN endpoints must freely exchange UPD traffic on ports 500 (ISAKMP) and 4500 (NAT traversal). Configure your network routers to forward incoming requests to VPN endpoints.
5. To avoid IP address conflicts and routing issues between VPN endpoints the internal network addresses of your sites must not cross.

VPN endpoint configuration for sites deployed on the premises

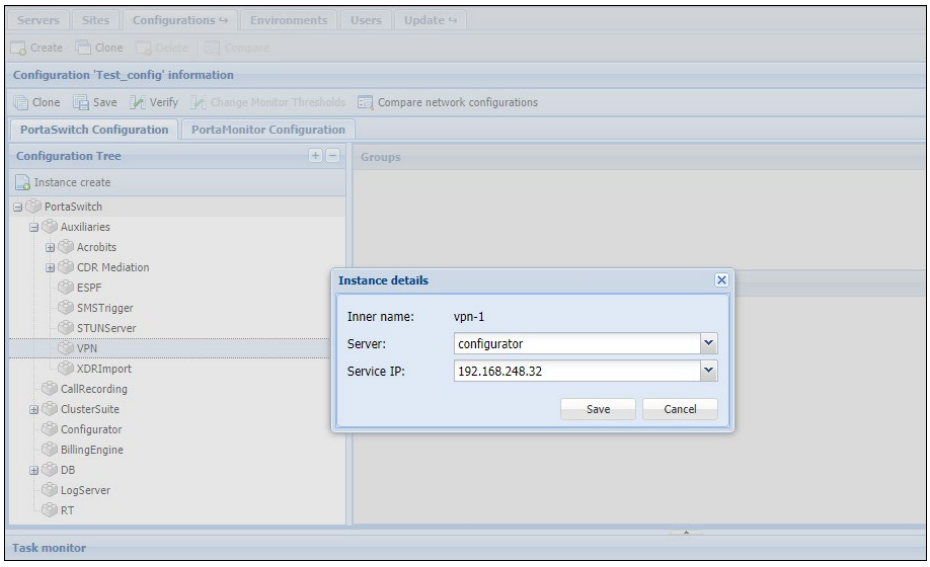
To configure a VPN endpoint for a site deployed on the premises you must obtain the following information about local (where you configure the endpoint) and remote sites:

- The VPN endpoint's public IP address
- The VPN endpoint's private IP address

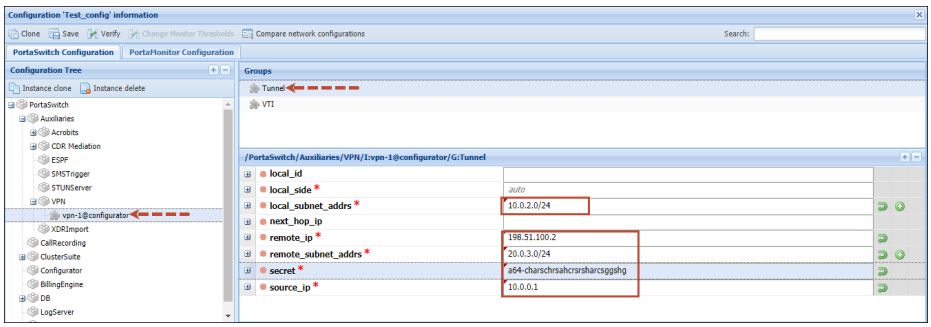
- The site's internal network address
- The pre-shared key used for authentication. You can generate a pre-shared key with openssl, pwgen or any other tool that can generate random string.

Complete the following steps:

1. Clone the existing configuration.
2. From the Configuration tree, select **Auxiliaries -> VPN**
3. Press the **Instance create** button.
4. Fill in the Instance create form:
   - **Server** – Select the server where the VPN instance will reside.
   - **Service IP** – Select the public IP address for the VPN instance.
5. Click **Save**.



6. Select the **Tunnel** group and fill in the following details:
   - **source_ip** – Specify the private IP address of the server with the VPN instance (e.g. 10.0.2.10).
   - **local_subnet_addrs** – Specify the internal network address of the local site (e.g. *10.0.2.0/24*). Click the icon to add more subnets.
   - **remote_ip** – Specify the public IP address of the remote VPN endpoint (e.g. *198.51.100.2*).
   - **remote_subnet_addrs** – Specify the internal network address of the remote site (e.g. *20.0.3.0/24*). Click the icon to add more subnets;
   - **local_side** – This is used to determine the VPN tunnel sides – left and right. Leave the default *auto* option for the system to automatically set the sides.
   - **secret** – Specify the pre-shared key used for authentication.



7. Click **Verify** to verify the configuration.
8. Click **Check/Apply** to apply the configuration.

Repeat these steps to configure the VPN endpoint on the remote site.

VPN endpoint configuration for sites hidden behind NAT

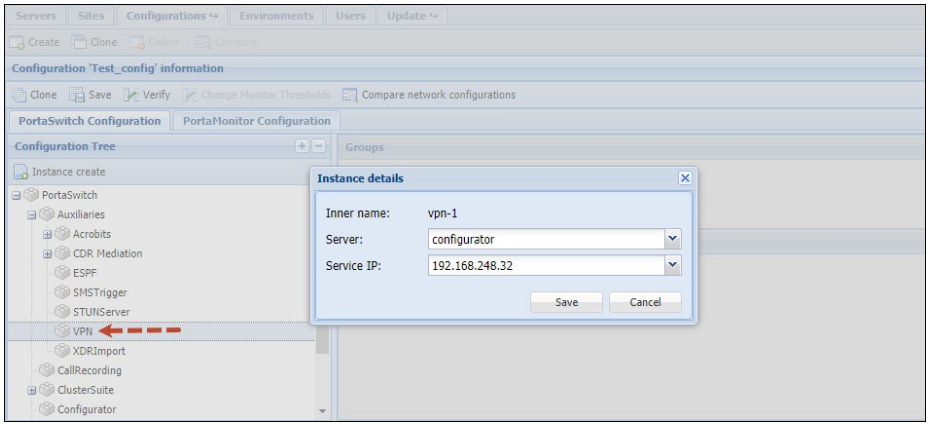
In this deployment, VPN endpoints can be allocated private IP addresses. However, NAT routers must be configured to forward incoming UDP requests to the VPN endpoint on ports 500 (ISAKMP) and 4500 (NAT traversal).

To configure a VPN endpoint for a site deployed on the premises you must obtain the following information about local (where you configure the endpoint) and remote sites:

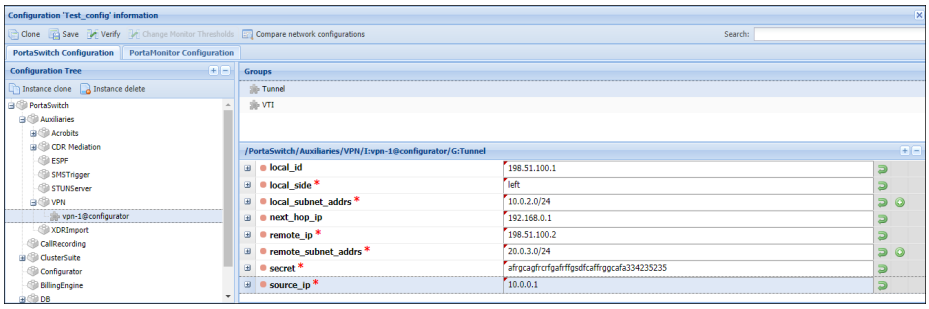
- The VPN endpoint public IP address;
- The VPN endpoint's private IP address;
- The NAT server's public IP address;
- The NAT server's private IP address
- The site's internal network address;
- The pre-shared key used for authentication. You can generate a pre-shared key with openssl, pwgen or any other tool that can generate random string.

To configure a VPN endpoint, complete the following steps:

1. Clone the existing configuration.
2. From the Configuration tree, select **Auxiliaries -> VPN**
3. Press the **Instance create** button.
4. Fill in the Instance create form:
    - **Server** – Select the server where the VPN instance will reside.
    - **Service IP** – Select the private IP address for the VPN instance.



5. Click **Save**.
6. Select the **Tunnel** group and fill in the following details:
    - **local_id** – Specify the public IP address of the local NAT server here (e.g. *198.51.100.1*).
    - **source_ip** – Specify the private IP address of the server with the VPN instance (e.g. *10.0.2.15*).
    - **local_subnet_addrs** – Specify the internal network address of the local site (e.g. *10.0.2.0/24*). Click the icon to add more subnets.
    - **next_hop_ip** – Specify the internal IP address of the local NAT server (e.g. *192.168.0.1*).
    - **remote_ip** – Specify the public IP address of the remote NAT server (e.g. *198.163.100.2*).
    - **remote_subnet_addrs** – Specify the internal network address of the remote site (e.g. *20.0.3.0/24*). Click the icon to add more subnets.
    - **local_side** – This is used to determine the VPN tunnel sides – left and right. Leave the default *auto* option here.
    - **secret** – Specify the pre-shared key used for authentication.



7. Click **Verify** to verify the configuration.
8. Click **Check/Apply** to apply the configuration.

Repeat these steps to configure a VPN endpoint on the remote site.

VPN endpoint configuration for sites deployed in a cloud

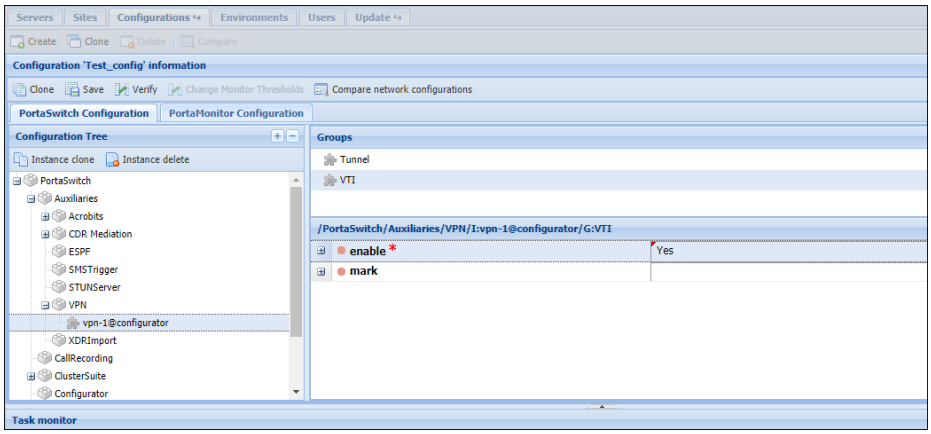
To set up a VPN endpoint for a site deployed in a cloud, the following information about your on-premises site is required:

- the public IP address for a remote VPN endpoint located on the premises;
- the IP address for the private on-premises network that will be added to the VPN.

The VPN endpoint configuration is handled by PortaOne Support. Once a VPN endpoint is configured in a PortaSwitch® Cloud network, you will be provided with its public IPv4 address, a pre-shared key and a private cloud network address.

To configure the VPN endpoint for your on-premises site:

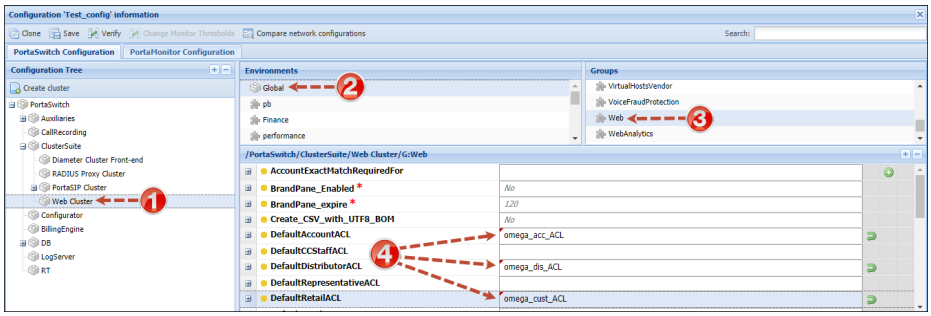
1. Create and configure the VPN instance as described in the **VPN endpoint configuration for sites deployed on the premises** section.
2. Enable the VTI mode for the endpoint:
   - Select the VTI group for the VPN instance;
   - Set **Yes** in the enable option.



3. Click **Verify** to verify the configuration.
4. Click **Check/Apply** to apply the configuration.

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

... Define new default ACLs



1. Clone the current configuration.
2. In the **Configuration Tree**, select the **Web Cluster** node.
3. In the **Environments** panel, select the environment in which you want to override default ACLs.
4. In the **Groups** panel, select **Web**.
5. Define one or more of the following options by typing the names of the ACLs that you created on the PortaBilling® admin interface:
    - **DefaultAccountACL** – Type the name of the account entities ACL.
    - **DefaultCCStaffACL** – Type the name of the CC Staff entities ACL.
    - **DefaultDistributorACL** – Type the name of the distributor entities ACL.
    - **DefaultRepresentativeACL** – Type the name of the representative entities ACL.
    - **DefaultRetailACL** – Type the name of the customer entities ACL.
    - **DefaultVendorACL** – Type the name of the vendor entities ACL.
    - **DefaultWholesaleACL** – Type the name of the reseller entities ACL.
6. Click the **Verify** button.
7. Verify the new modified configuration and apply this configuration.

Note that you can always make the original PortaBilling® predefined ACL visible and available again by clicking the **Reset** button near the corresponding option.

… Delete an active billing environment?

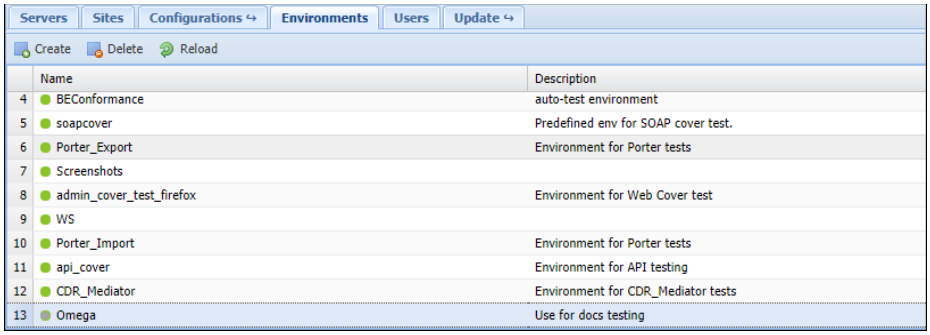
A billing environment is considered to be *active* if its configuration includes at least one instance of

- PortaSIP®
- SIPCluster
- IMGate
- Presence

Active billing environments are in read-only mode and cannot be deleted.

NOTE: The name of an active environment is marked with a grey circle on the web interface, while the name of a non-active environment is marked with a green circle.

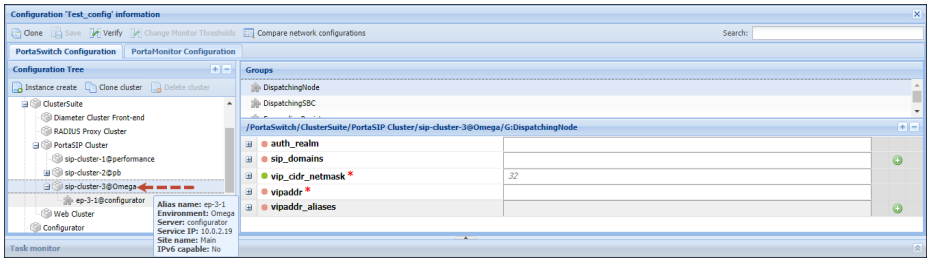
All of the instances mentioned must be deleted prior to deleting the environment. This is to ensure that no PortaSIP®, IM or presence services are running.



In order to delete an active billing environment proceed with the following steps:

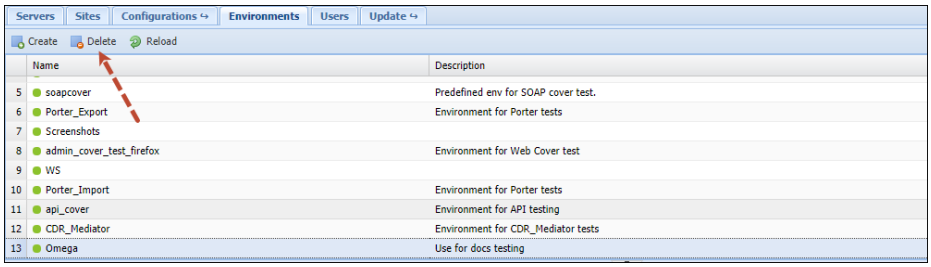
1. Go to the **Configurations** tab and clone the latest configuration.
2. Open the cloned configuration. In the **Configuration Tree** select the PortaSIP® instance from the required billing environment and click the **Instance delete** button. Repeat for all PortaSIP®, SIPCluster, IMGate and Presence instances.

   NOTE: Deletion of PortaSIP® instances instantly deactivates all PortaSIP® services in the corresponding billing environment.



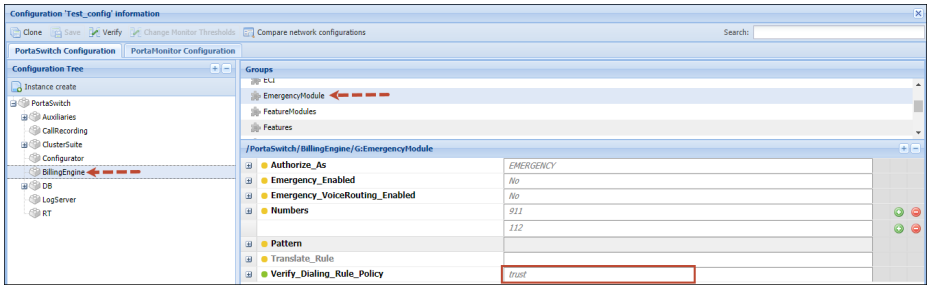
3. When all required instances have been deleted, click the **Verify** button. Then, click the **Check/Apply** button to apply the given configuration.
4. Go back to the **Environments** tab. Select the environment that you want to delete. Press **Delete**.

NOTE: Be aware that once the environment is deleted, all of its settings (tariffs, customers, accounts, vendors, connections, etc.) and CDRs are removed from the PortaBilling® database. You will only have access to statistics in .csv format.



… Enable additional validation of dialing rule emergency numbers?

The system can perform an additional validation of emergency numbers that are specified in the dialing rule. To enable such a validation, use the **Verify_Dialing_Rule_Policy** option on the Configuration server web interface (**BillingEngine→Emergency_Module**).



This option can have one of the two values:

- **trust** – Emergency numbers specified in a dialing rule won't be validated.
- **check** – System will check that emergency numbers specified in a dialing rule are among the numbers listed in the **Numbers** option or comply with the rule specified in the **Pattern** option.

The default value is **trust**. If you want to validate dialing rule emergency numbers, select **check** and specify which numbers and / or pattern the numbers must match.

This can be useful if you enable end users to configure their own dialing rules and want be sure that they won't use unsuitable emergency numbers.

Depends on: **EmergencyModule.Emergency_Enabled**.

… Migrate an instance?

The procedure of instance migration is similar for all instance types, although some types have their own particularities. The procedure itself may vary, depending on whether this is a scheduled operation or an urgent recovery after a server failure.

In this chapter we will show you how to migrate an instance from one physical server to another as part of a scheduled operation. We will assume that on a new server you will use a new IP address for the migrated instance.

1. (Optional) Go to the **Servers** page and create a new server.
2. On a target (new) server add a dedicated IP address to be used for the migrated instance.
3. Create a new configuration (referred to as **Configuration A** later on) as a clone of the currently active configuration:
    - Clone the currently active configuration.
    - Delete old instances that are to be migrated from the former server.
    - Save and close this new configuration but *do not* yet apply it.
4. Create another new configuration (referred to as **Configuration B** later on) as a clone of the currently active configuration:
    - Clone the currently active configuration.
    - Modify instances that are to be migrated to the target server:
        - Select the instance and click **Update Instance**.
        - Select a new server on which this instance will run.
        - Specify a new Service IP.
        - Press **OK**.
    - Save and close this new configuration but *do not* yet apply it.
5. Check and apply both new configurations one by one (**note that service downtime is required to apply changes**):

- Open **Configuration A** and click the Verify button to make sure that it contains all the required changes and that no unwanted options were modified by mistake. Then, click the **Check /Apply** button to verify if the configuration is valid.
- When the check is done click the **Apply** button.
- Close C**onfiguration A**.
- Open C**onfiguration B** and click the **Verify** button to make sure that it contains all the required changes and that no unwanted options were modified by mistake. Then, click the **Check /Apply** button to check if the configuration is valid.
- When the check is done click the **Apply** button.

The Configuration server will apply the new configurations by performing the following steps:

1. **Configuration A**:
   - New IP addresses will be added to the target server.
   - Instances will be removed from the former server.

2. **Configuration B**:
   - Instances will be created and started on a target server.

Useful tips

Make sure to consider the following tips:

- Some instance types cannot run from one server (see the **Add Instances** section for more details).
- If the log server is configured, it will continue writing log files for the migrated instance, otherwise new log files will be created on the target server.
- If you have a web cluster then you can migrate web instances one by one without initiating a service outage, otherwise use the **migration plan** above for web instance migration.
- To migrate a DB instance (either Master DB or Replica DB) you need to manually copy the database (e.g. using a snapshot) to a target server and then update the instance using the **migration plan**.

Note that you may want to set up replication from the currently active database to the new one (e.g. configure the *currently active Master DB→New Master DB→Replica DB* replication when the copy process is finished) to keep the services running while the database is being copied. This decreases the services outage time during the migration. If you do this, then do *not* forget to stop the services and the replication just before applying the new configurations.

... Migrate an IP address?

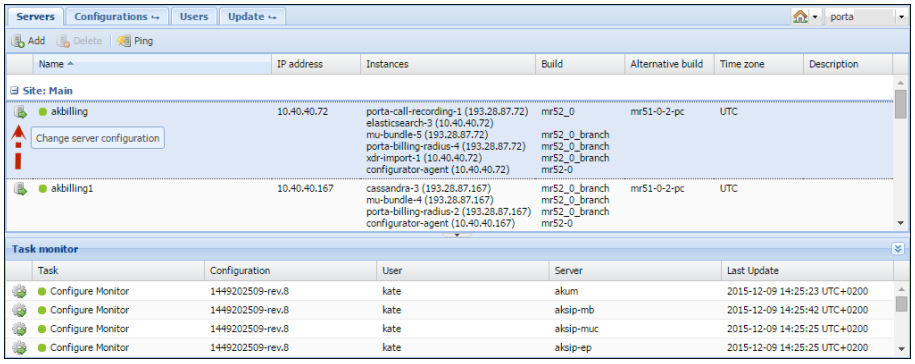
If you want to re-assign an IP address from a given server or installation to another, you need to complete the IP address migration procedure. It includes the deletion of an IP address from one given server or installation and adding it to another one.

NOTE: Make sure that the IP address you delete is no longer in use. Otherwise the changes will not be applied to the new installation.

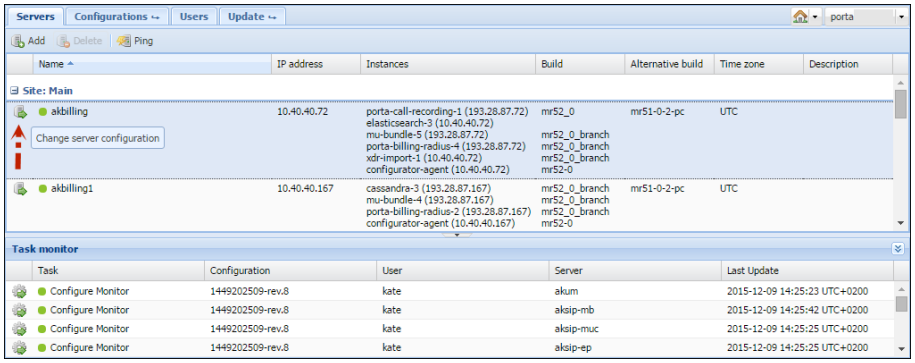
How to delete an IP address

To delete an IP address, complete the following steps:

5. Go to the **Servers** tab.
6. Select the server from which you want to delete an IP address and click on the **Change server configuration** icon on the left-hand side of the server's name.



7. Click **Get configuration** to update the network configuration.
8. Click on the required IP address. This activates the **Delete** button. Click on **Delete → IP address**. Now the IP address is removed from this server.



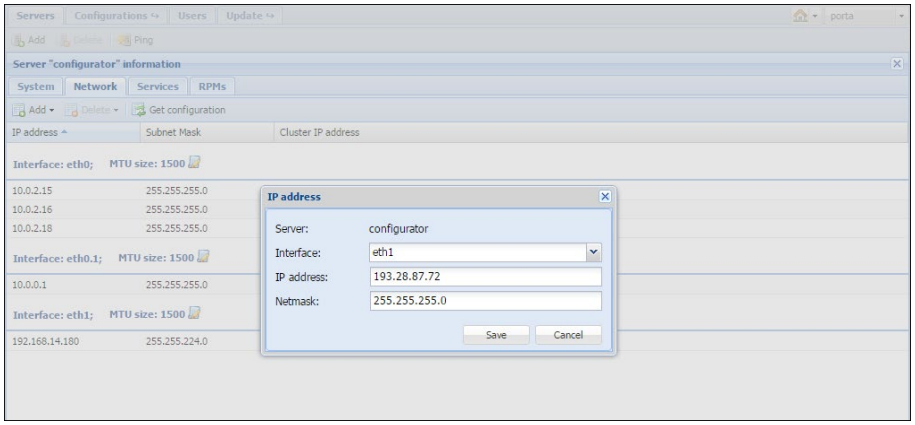
9. Go to the **Configurations** tab.

10. Clone the active configuration and verify the changes. Then, click **Check/Apply** to apply the configuration.

How to add an IP address

To add an IP address to a server, complete the following steps:

1. Go to the **Servers** tab.
2. Select the required server and click on the **Change server configuration** icon on the left-hand side of the server's name.
3. Click **Get configuration** to update the network configuration.
4. Click on **Add → IP address**. In the **IP address** dialog box, specify the following information:
   - **Interface** – Select the required interface from the list.
   - **IP address** – Type in the IP address you want to add.
   - **Netmask** – Type in the netmask for the given IP address.



5. Click **Save**.
6. Go to the **Configurations** tab.
7. Clone the active configuration and verify the changes. Then, click **Check/Apply** to apply the configuration.

5. Appendices

APPENDIX A. Internal modules of the billing engine

Below you will find the descriptions of some modules that allow you to enable or disable certain PortaSwitch® features. We suggest that you enable additional modules (that have been disabled by default) *only* if you understand how they work and plan to use the functionality they provide.

NumberPortability

This feature is enabled on the Configuration server by default.

See the *Local Number Portability* section in the **PortaBilling Administrator Guide** for more information about this feature.

CallParking

This is a convenient IP Centrex feature that allows users to put a conversation on hold, move to a different location, and then resume the conversation from a different IP phone by dialing a pickup code. Enable **Call Parking** when you want to use this feature.

GroupPickup_Enabled

By dialing a Group Pickup Prefix on the phones, this feature permits those phones within the same IP Centrex environment (all accounts under the same customer) to answer each other's calls. This feature is enabled by default.

FavoriteNumbers_Enabled

The **Favorite numbers** feature permits the application of a special promotional rating for a group of numbers that are individually defined for each subscriber. After this feature is enabled in the billing engine, the "Favorite numbers" feature is enabled for individual accounts on the **Account info** page in the **Service Features** tab of the web interface.

Callback

Enabling this module permits the use of the special authorization and rating models for callback service.

DialPlan_Enabled

This module is used to produce a "routing prognosis" (a list of routes to be used when a specific phone number is called) when requested from the

"Test dialplan" portion of the PortaBilling web interface. It should be enabled in order for the web dial plan component to operate correctly.

CLDlookupInDIDinventory (DID Inventory Module)

If you purchase bulk numbers from a telco operator and upload them to PortaSwitch®, but some of them are not yet provisioned to PortaSwitch® accounts, these numbers may cause routing loops. Someone calls a number; the call is delivered to your network; but since the destination number does not belong to any local account, PortaSwitch® considers it to be an outside number and routes it to an external carrier, which then delivers it to your network again, and the action repeats continually, again and again.

In order to prevent this from happening, numbers that do not belong to any local accounts (while currently available in the database) can be "registered" in the DID inventory. When a call is made to one of these numbers, PortaSwitch® considers these numbers "not yet provisioned" and therefore, the call fails and shows the following disconnection code: CLD_UNASSIGNED. Therefore, enable this module to prevent routing loops for calls to unassigned DID numbers.

UnifiedMessaging_Enabled

When this module is enabled it takes control of the handling and routing for the PortaSwitch® Media server voice applications. Do not forget to activate the UM feature for products that are required to provide UM service:

1. On the PortaBilling® **Main Menu** page, in the **Rating** section, choose **Products**.
2. On the **Product Management** page, click on the name of the corresponding product.
3. Click on the **Service Configuration** tab.
4. In the **Services** column, under **Voice Calls**, select **Incoming Calls**.
5. From the **UM Enabled** list, select **Enabled** to activate UM services for this product.

IvrUtilities_Enabled

This module implements various actions, requested by IVR applications (e.g. performing a customer sign-up by creating a new account). This module is enabled on the Configuration server by default.

Paging_Enabled

PortaSwitch® supports the Paging / Intercom Calls feature, which enables users from the same group to use two phones like an on-door speakerphone.

This module is enabled on the Configuration server by default.

See the **Paging / Intercom Calls** section in the **PortaSIP Administrator Guide** for more information.

FixUpBrokenAccessNodeRatingPatterns

Enable this module if you need a workaround for improperly configured third party nodes, i.e. when one node sends a call to another one in a non-E.164 format and the BE authorization is inconsistent with access code accounting.

NOTE: When using the rating pattern on third-party access nodes, no newer special features will be available.

APPENDIX B. Paths to tops of build areas in SRPM packages

The following table provides paths to the tops of build areas for patching SRPM packages. For example, to modify `/opt/diaconv/file` specify the `./diaconv/file` path in a patch file's header.

SRPM	The Path on the File System	The Path in a Patch File
archivist	/home/archivist/file	./file
b2bua	/home/porta-sip/sippy/file	./file
checksuite	/usr/share/suitability-checker/file	./file
dbup	/home/porta-configurator/pcup/dbup/file	./file
dbup2	/home/porta-configurator/pcup/dbup2/file	./file
diaconv	binary	./file
edgeproxy	binary	./file
extractaudio	binary	./file
fopd	binary	./file
g729client	binary	./file
g729d	binary	./file
imgate	binary	./file
libg723-devel	binary	./file

libg729-devel	binary	./file
libilbc-devel	binary	./file
liblog	binary	./file
limit-controller	binary	./file
log4cplus-python	binary	./file
makeann	binary	./file
oracle-encrypt	binary	./file
porta-admin	/home/porta-admin/file	./file
porta-base	/home/porta-base/file	./file
porta-billing	/home/porta-billing/file	./file
porta-callrecording	/home/porta-callrecording/file	./file
porta-cdrimport	/home/porta-cdrimport/file	./file
porta-cdrmediator	/home/porta-cdrmediator/file	./file
porta-configurator	/home/porta-configurator/file	./file
porta-configurator-data	/home/porta-configurator/data/file	./file
porta-db	/home/porta-db/file	./file
porta-ivr	/home/porta-ivr/tcl/file	./file
porta-ivr-tts	/home/porta-ivr/tts/file	./file
porta-monitor	/usr/libexec/nagios/portaone/file /var/www/nagios/rrd/file /etc/nagios/file	./config/file ./plugin/file ./rrd/file
porta-mp-signup	/home/porta-admin/apache/multi_product_signup/file	./file
porta-mysql	/usr/lib/systemd/system/porta-mysqld.service	./porta-mysqld.service
porta-oracle	/home/oracle/file	./file
porta-presence	/home/porta-presence/file	./file
porta-radius	/home/porta-radius/file	./file
porta-rt	/home/porta-rt/file	./file
porta-selfcare	/home/porta-admin/apache/IPCentrex_SelfCare/file	./file
porta-signup	/home/porta-admin/apache/signup/file	./file

porta-sip	/home/porta-sip/file	./file
porta-smstrigger	/home/porta-smstrigger/file	./file
porta-um	/home/porta-um/file	./file
porta-ws	/home/porta-ws/file	./file
protector	/home/protector/file	./file
registrar	binary	./file
runtest	/home/porta-one/billing-performance/file	./file
siplogindexer	binary	./file
sip-prompts	/var/lib/porta-sip/sounds/file	./file
sip-subscription-manager	binary	./file
ua-profile-gen	/home/porta-admin/utils/ua/file	./file
um-prompts	/var/lib/psmsc/prompts/file	./file
wssetup	/usr/share/wssetup/file	./file