PORTA ONE

PortaSwitch

# Installation Guide

MAINTENANCE RELEASE 80

www.portaone.com

# Copyright Notice & Disclaimers

**Copyright © 2000–2020 PortaOne, Inc. All rights reserved**

**PortaSwitch® Installation Guide, February 2020**
**Maintenance Release 80**
**V1.80.03**

Please address your comments and suggestions to: Sales Department, PortaOne, Inc. Suite #408, 2963 Glen Drive, Coquitlam BC V3B 2P7 Canada.

Changes may be made periodically to the information in this publication. The changes will be incorporated in new editions of the guide. The software described in this document is furnished under a license agreement, and may be used or copied only in accordance with the terms thereof. It is against the law to copy the software on any other medium, except as specifically provided for in the license agreement. The licensee may make one copy of the software for backup purposes. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopied, recorded or otherwise, without the prior written permission of PortaOne Inc.

The software license and limited warranty for the accompanying products are set forth in the information packet supplied with the product, and are incorporated herein by this reference. If you cannot locate the software license, contact your PortaOne representative for a copy.

All product names mentioned in this manual are for identification purposes only, and are either trademarks or registered trademarks of their respective owners.

## Table of Contents

# Preface

This document provides a general overview of the installation process for the PortaSwitch 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.

**Archivist** explains how the feature worked in previous releases.

**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.

# 1. Introduction

All the servers are identically installed from the same set of installation media (of course you should specify unique IP addresses, host names, etc. for each server). Follow the steps given in the **Installation process** chapter of this guide to perform the server installation. The assignment of roles (e.g. PortaBilling® RADIUS, PortaBilling® admin interface, PortaSIP®, etc.) will be done in Step 16 after all hosts have been installed.

The installation media provide a quick and seamless way to perform a complete server installation from scratch in less than 15 minutes. The standardized installation procedure also simplifies further system maintenance.

PortaOne provides you with two ISO files (Disc 1 and Disc 2) that contain the following software required for installing PortaSwitch®:
- The Telecom Application Framework (free, open-source software) – required to install Oracle Enterprise Linux 7.5 (Disc 1).
- The PortaSwitch® (PortaOne's proprietary software) – contains PortaSwitch® packages (Disc 2).

Burn these files to the optical discs or use them to create bootable USB flash drives. For additional help on how to create a bootable USB flash drive check the **... create a bootable USB flash drive from a PortaSwitch® ISO file?** section of the **How to...** chapter of this guide.

The installation wizard makes use of a GUI. Use the mouse or **Tab** to move the cursor between input fields, click on a button to confirm your selection.

# Hardware and software requirements

## Compatibility CD

If you want to determine whether PortaSwitch® can be installed on a specific server, please use the **Hardware compatibility** tool provided by PortaOne.

Note that this procedure will remove all data from your hard disk drive.

You can download the ISO file with the **Hardware compatibility** tool from:

**http://portaone.com/resources/hw_test/HardwareCompatibilityCD.iso**

Burn it to an optical disc or create a bootable USB flash drive from it, then boot up from this medium. The PortaSwitch® test utility will detect if all of the required components (e.g. network interface) are available and supported by Linux.

## Hardware requirements

Make sure that your servers are installed and equipped with all the required hardware, in particular:

- A 64-bit processor (Xeon, Opteron) released in 2010 or later, with frequency of 2.2GHz or higher. Additional processors are recommended for networks with a high call volume.
- At least 250 GB of the total available disk space.
- Two network (Gigabit Ethernet) ports.
- DVD-ROM – if you want to install PortaSwitch® from optical discs (in the case of a USB DVD-ROM, follow the steps in the **... install PortaSwitch® using USB DVD-ROM?** section of the **How to...** chapter to start the installation) or USB slot – if you want to install PortaSwitch® from USB flash drives.
- Video adapter / monitor / keyboard / mouse (required only during the installation process).

Please avoid any entry-level or desktop-oriented components – use only high-performance ones. For example, RAID must be write cache enabled, network adapter must be the "server" mode. Check if the hardware installed on your server is supported by Oracle Enterprise Linux 7.5. You can check this at the website: **http://hardware.redhat.com**.

## Network configuration parameters

During the installation you will be prompted for the network configuration parameters. Please make a decision regarding these before installation, consulting your network administrator if necessary. It is possible that you will have to perform installation while the network is not yet available (from your office, for example, while the servers will be placed in a server hosting center), but you will need to enter the correct data anyway. Please have the following ready:

- Planned host names and IP addresses of the servers.
- Subnet mask.
- IP address of the default gateway.
- IP address of the DNS server.

### RAID configuration

If you have a hardware RAID controller in your system, please configure it by creating a logical RAID entry and allocating the physical drives to it. The recommended configuration (depending on the amount of hard drives in the system) is as follows:

- 2 disks – RAID 1 (mirroring).
- 3 disks – RAID 1 (mirroring) on the first two disks, third one left as a hot spare.
- 4 disks – RAID 1+0 (mirroring + striping).
- More than 4 disks – RAID 1+0 (mirroring + striping) on the first four disks, others left as a hot spare.

# 2. Network configuration

The figure below shows a common network configuration for PortaSwitch®.
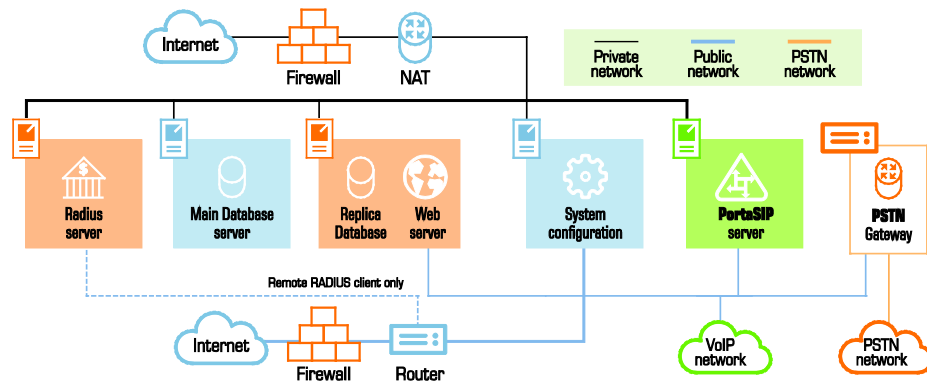


PortaSwitch® server requires two physical network interfaces:

- The first network interface is connected to a private LAN segment for internal communication between servers (the black lines on the diagram). Private LAN must allow servers to initialize outgoing connections to the Internet (using NAT) for the purposes of monitoring, performing maintenance and updating the servers.
- The other network interface is connected to the public Internet segment. This interface is used to provide "public" services (such as VoIP calls or access to the self-care portal) to your customers. This public Internet connection is marked by the blue lines on the diagram.

> **NOTE:** If all servers can initialize outgoing connections to the Internet via the public Internet segment, there is no need to configure an outgoing connection for a private LAN.

Two physical network interfaces are required for the following purposes:

- Improved network security, since all data (such as access to the database or the transfer of sensitive customer information) is transported via a dedicated interface.
- Ability to quickly and easily relocate services (including public IPs allocated to each service) from one physical server to another, or to change the roles of the servers.
- In case public IPs are not accessible anymore (e.g. the servers have been physically moved to a different hosting facility, or the administrator supplied incorrect information regarding a public IP), it is still possible to access the server via the internal interface and fix the configuration.
- Intensive data transfer on one interface (e.g. database copy for a daily backup) does not affect services provided on the other interface (e.g. media transport for voice calls).

Consider the following when planning your network:

- Private IP addresses must be in the same LAN (or VPN).
- RADIUS servers do not normally require a connection to the public Internet segment, so it is recommended that you not assign public IP addresses to them. The only exception is when you have remote RADIUS clients which cannot interconnect with RADIUS servers via private IP addresses. Below you will find the parameters that must be configured when you only assign private IP addresses to RADIUS servers. This is usually done by the PortaOne support team once the system has been installed:

  If you only assign private IP addresses to RADIUS servers then you must specify a RADIUS server's private IP address in the **RadiusClient.Source_Address** option on the Configuration server web interface.

  If you are installing a RADIUS cluster, then the **RADIUS.Forward_Mode** option on the Configuration server web interface must also be enabled. This allows the RADIUS requests to be relayed to all of the RADIUS servers when you specify the private IP address for only one of them in the above options.

- Additional processes (e.g. geo-IP database auto-update or real-time lookup in a central LNP database) may run on the RADIUS servers if respective features are enabled (even if they do not relate to the RADIUS protocol.) These processes may require outgoing connections to specific IP addresses or to the whole public Internet: direct, via NAT or via different sorts of custom proxying.
- Dedicated database servers do not require a connection to the public Internet segment, so it is recommended not to assign them public IP addresses.
- If you are planning to pass PCI DSS compliance, you should have dedicated databases with only private IP addresses. These IP addresses must be on a separate subnet.

Although not all servers need to be assigned IP addresses from the public Internet segment, we recommend that a physical connection be established for all servers (then you can easily swap roles between the servers using PortaSwitch® configuration tools).

You can find our recommendations regarding the firewall in the **What is the Recommended Setup for the PortaSwitch® Behind a Firewall?** section of the **Frequently Asked Questions** chapter.

You may configure virtual interfaces (VLANs for trunking) and / or network bonding (link aggregation) for servers using the Configuration server. For more details see the **PortaSwitch Configuration Server Web Reference Guide**.

# 3. Installation process

# Step 1: Power-up, boot order setup

1. Turn on the computer which you plan to use as the server.
2. Enter the BIOS setup and make sure that the device you are going to use for installing PortaSwitch® is on the top of the boot list.
3. In case you want to use a USB flash drive, also check that USB support is enabled.

```
                    PhoenixBIOS Setup Utility
   Main      Advanced    Security     Power    Boot     Exit

                                              Item Specific Help

    ATAPI CD-ROM Drive
  +Removable Devices
  +Hard Drive                           Keys used to view or
                                        configure devices:
                                        <Enter> expands or
                                        collapses devices with
                                        a + or -
                                        <Ctrl+Enter> expands
                                        all
                                        <Shift + 1> enables or
                                        disables a device.
                                        <+> and <-> moves the
                                        device up or down.
                                        <n> May move removable
                                        device between Hard
                                        Disk or Removable Disk
                                        <d> Remove a device
                                        that is not installed.

  F1   Help    ↑↓  Select Item   -/+   Change Values   F9   Setup Defaults
  Esc  Exit    ←   Select Menu   Enter Select ▶ Sub-Menu F10  Save and Exit
```

**NOTE:** This image is only an example. The BIOS on your system might look different**.**

4. Save your changes and exit.

Beginning with MR50, PortaSwitch® supports UEFI (Unified Extensible Firmware Interface) – a standard firmware interface for PCs and servers designed to replace BIOS. If your servers use UEFI, we strongly recommend disabling the UEFI Secure Boot feature as it may prevent PortaSwitch® servers from booting up correctly.

There is a known issue that some Dell servers can't find a proper MBR when they boot up from the PortaSwitch® installation USB flash drive. The solution is to set the **USB Flash Drive Emulation Type** option to "Hard disk" in the BIOS setup. For more information, please refer to:
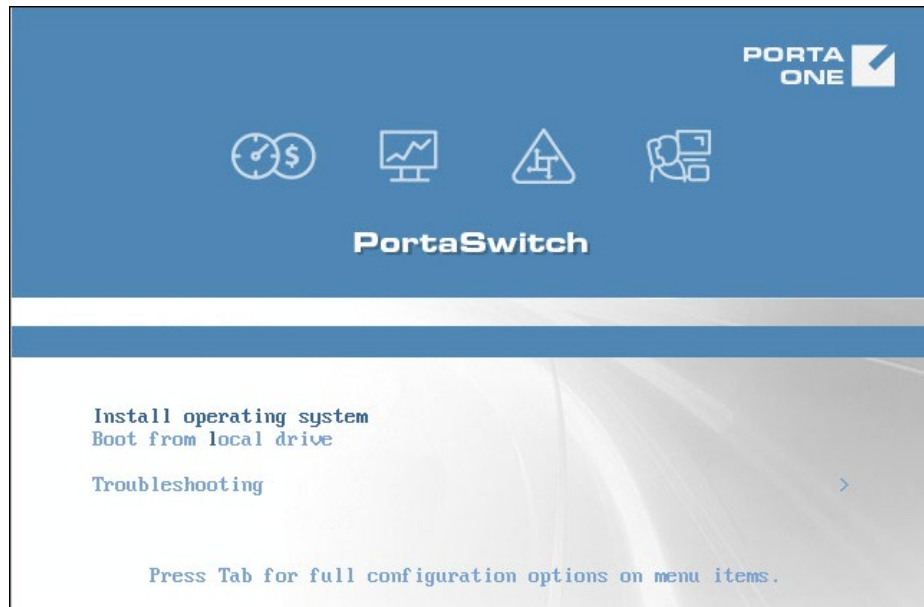
http://en.community.dell.com/techcenter/b/techcenter/archive/2012/02/29/hybrid-iso-images-on-dell-servers

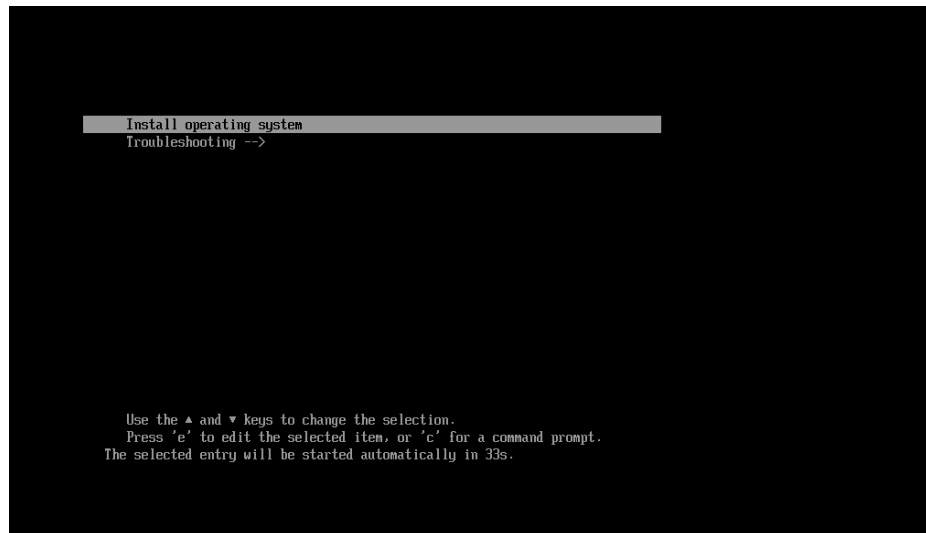# Step 2: Insert the installation medium into the computer

While booting the system, insert the installation medium (optical disc or USB flash drive) with PortaSwitch® installation Disc 1 into the computer. If you do not insert it soon enough, and get a "no operating system" error (or a previously installed operating system starts its boot-up process) then press **Reset** and ensure that you are booting from the proper device.

# Step 3: Starting installation

Successful boot-up from the installation media takes you to the **Installation Menu** page. Use the arrow keys, **Enter**, **Esc** and **Tab** keys to navigate it.

If you use UEFI, this screen will look the following way:



```
Install operating system
Troubleshooting -->




Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
The selected entry will be started automatically in 33s.
```

To start the installation of PortaSwitch® software do the following:
1. Choose the **Install operating system** option.
2. Press **Enter**.

**NOTE:** If you don't manually choose an option before the automatic boot countdown timer runs out, the server will continue to boot-up from the local disk. In this case, press **Reset** to reboot your system and return to the **Installation Menu** options.

If you completed this step but the installation process doesn't seem to be proceeding normally, check the **... perform basic troubleshooting?** section of the **How to...** chapter of this guide.

# Step 4: Installation summary page

In the next step of the installation process the **Installation summary** page appears:
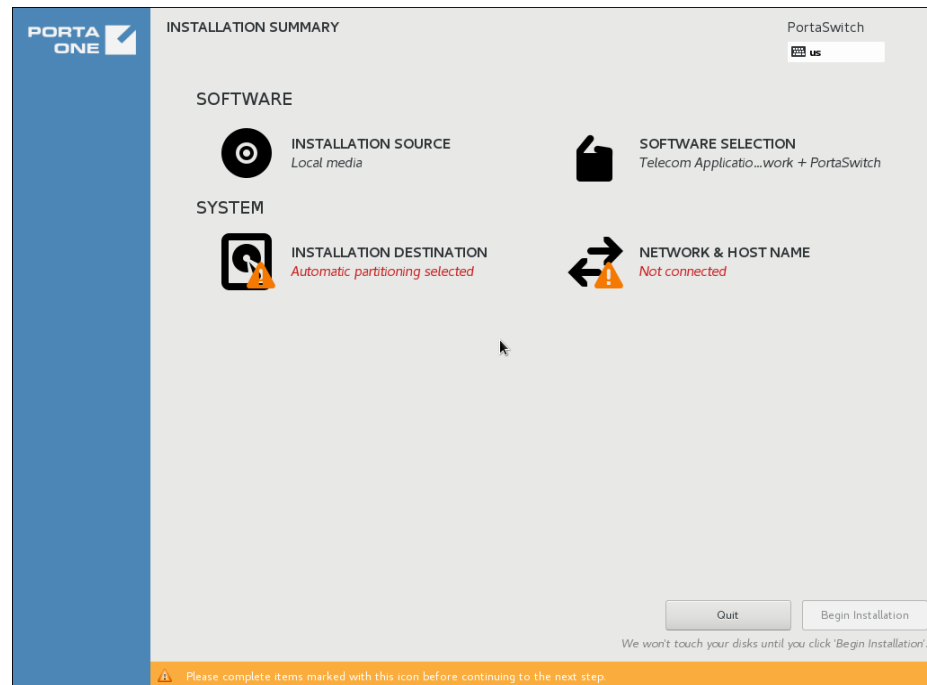
You need to complete four sections before you can proceed further with the PortaSwitch® installation. Two sections deal with the software that you install, providing the installation utility with information about where to install the software (**Installation source**) from, and which specific software package to use (**Software selection**). The other two sections allow you to configure your system parameters – what devices (disks) will the software be installed to (**Installation destination**) and which settings this software will use to communicate via the network (**Network & host name**).

From here on the uncompleted sections of the installation interface are marked with exclamation marks in yellow triangles. Additionally, at the bottom of the page there is a yellow ribbon that offers hints for what needs to be completed.

# Step 5: Installation source

In this step define where you want to install the PortaSwitch® software from:
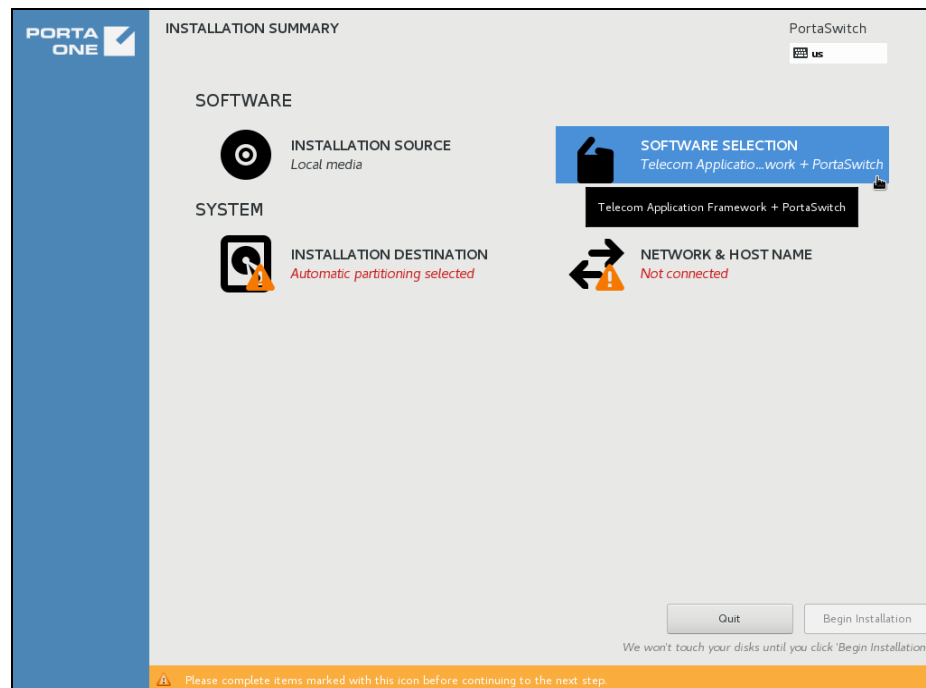
1. On the **Installation summary** page, choose **Installation source**.
2. Choose **Auto-detected installation media**.
   - You can click the **Verify** button to make sure that the ISO file wasn't corrupted during download or being burned to the installation medium. After the check finishes, click
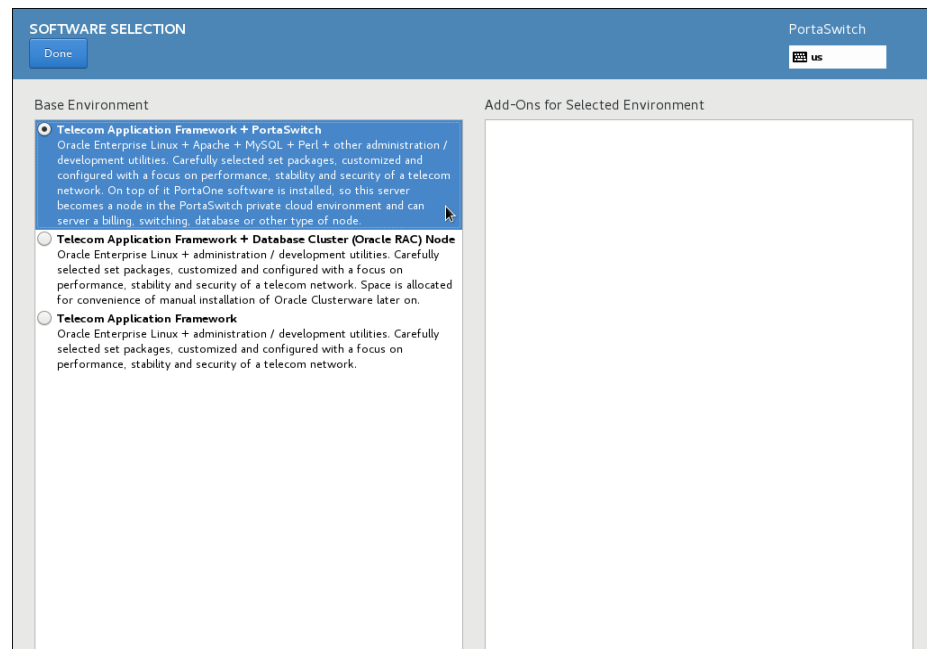
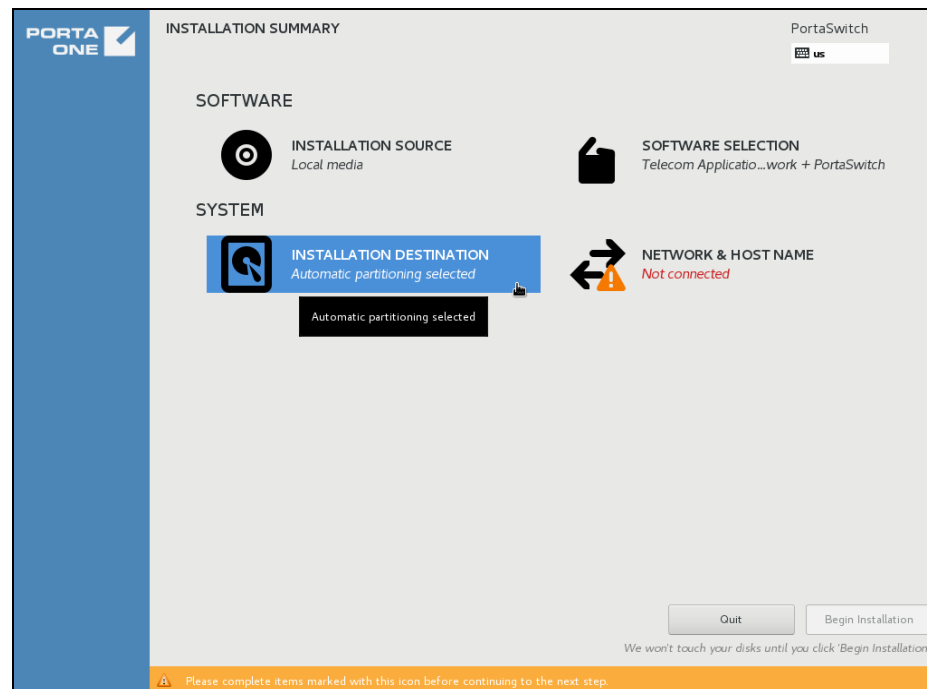**Done** on the bottom of the **Media verification** dialog window.
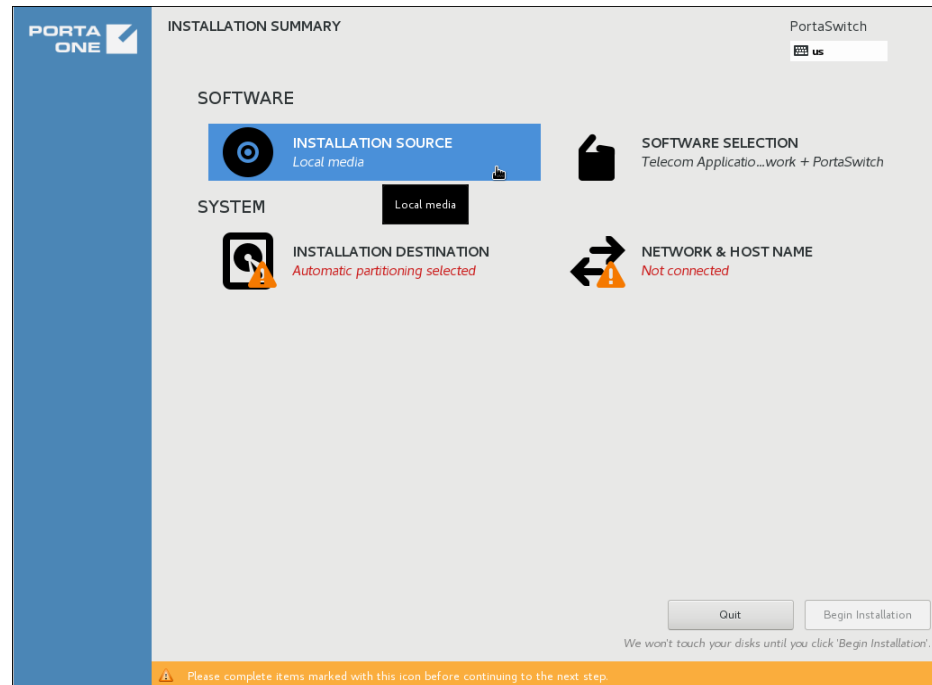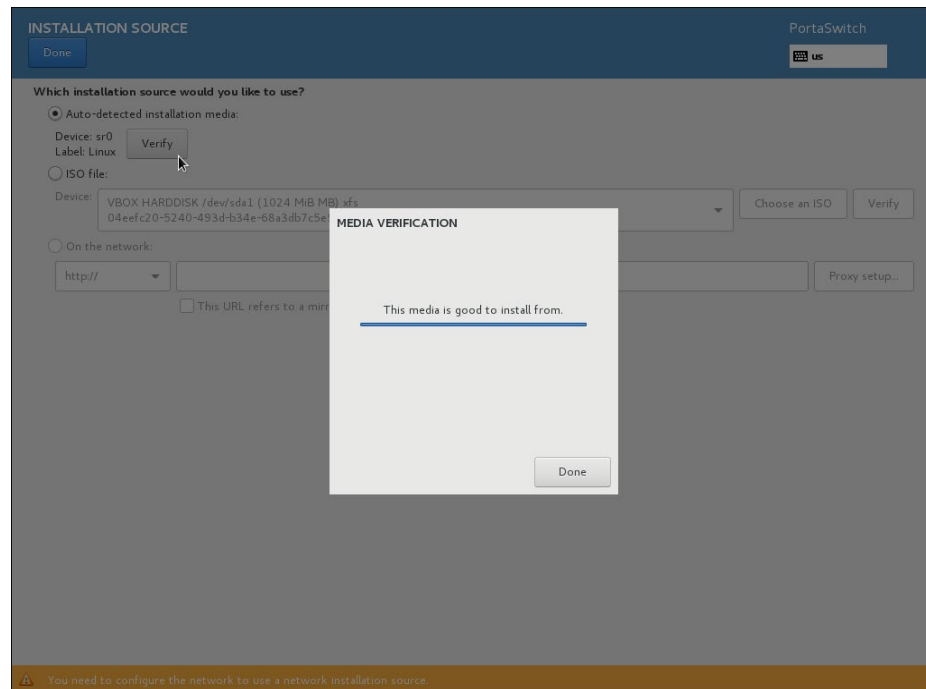
3. Click **Done**.

# Step 6: Software selection

1. On the **Installation summary** page, choose **Software selection**.
2. In the **Base Environment** section, choose **Telecom Application Framework + PortaSwitch**.
3. Click **Done**.

# Step 7: Installation destination

1. On the **Installation summary** page, choose **Installation destination**.
2. In the **Device Selection** section, go to the **Local Standard Disks** area, and select the local disk you want to install PortaSwitch® to. You can click the **Full disk summary and bootloader** link at the bottom left side of the page to see full information about each disk.
3. In the **Other Storage Options** section, go to the **Partitioning** area, and choose **Automatically configure partitioning**.

   **NOTE:** Although it is possible to manually alter the partition layout on the volume, unless you have a deep knowledge of PortaSwitch® architecture and a specific reason to make adjustments – do not alter the default partition layout as it can cause serious problems during future PortaSwitch® software upgrades.

   If you did choose to alter the default partition layout manually, you must select the LVM partitioning scheme. It is required for successful operation of PortaSwitch® and to perform future software upgrades.

4. Click **Done**.

   **NOTE:** Selected disks will be left untouched until you click the **Begin installation** button on the **Installation Summary** page.

# Step 8: Network & host name
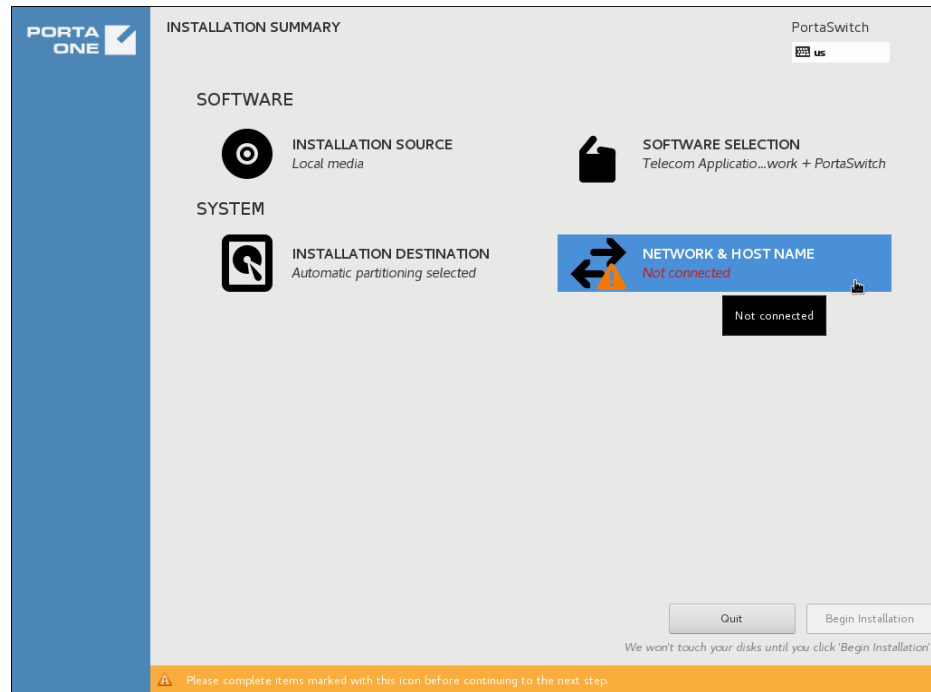


1. On the **Installation summary** page, choose **Network & host name**.
2. Specify a fully qualified host name for the current server.

   **NOTE:** The host name should not contain dashes.

3. Choose the network interface that is connected to a *private LAN segment* and click the **Configure** button.
4. Go to the **IPv4 Settings** tab.
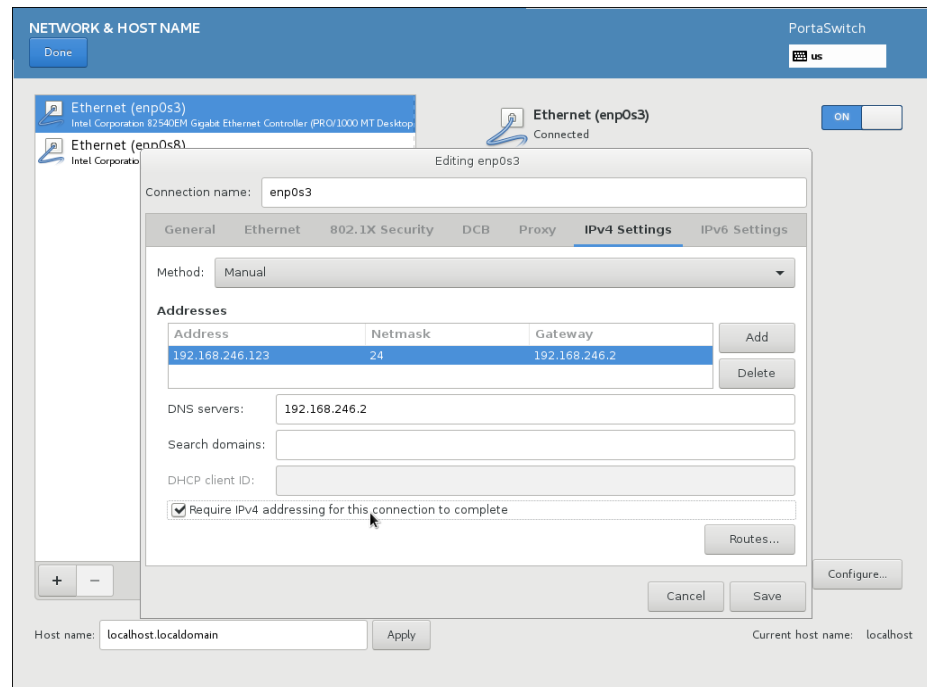
5. From the **Method** menu, choose **Manual**.
6. In the **Addresses** section, click the **Add** button and specify the following network details:
   - Private IP address that will be used for internal communications between servers
   - Network mask
   - Default gateway

7. Specify DNS servers. Use commas to separate multiple DNS server addresses.
8. Select the **Require IPv4 addressing for this connection to complete** checkbox.
9. Go to the **General** tab.
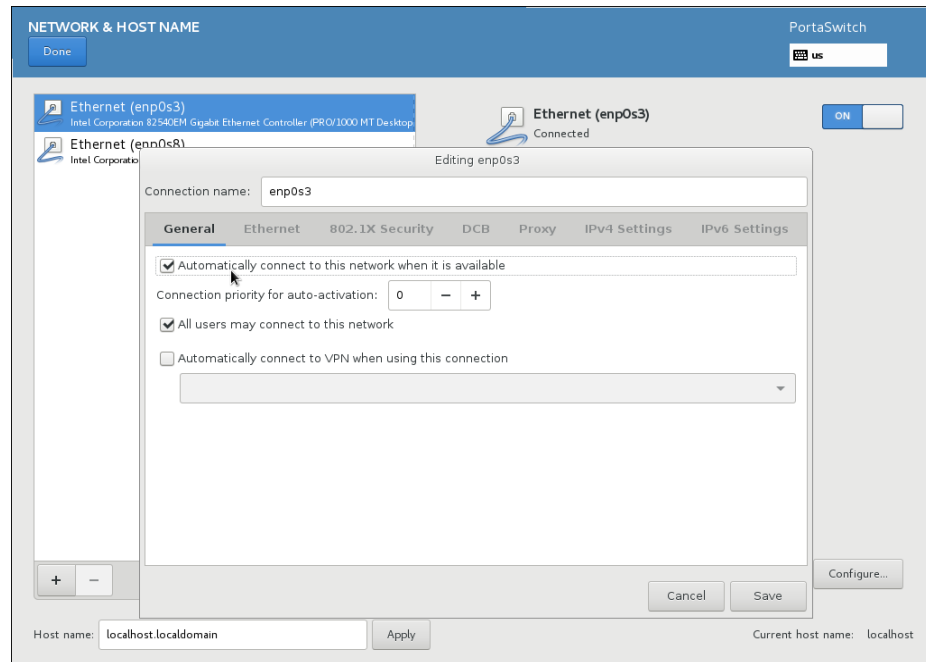
10. Select the **Automatically connect to this network when
    available** checkbox.
11. Click **Save**.
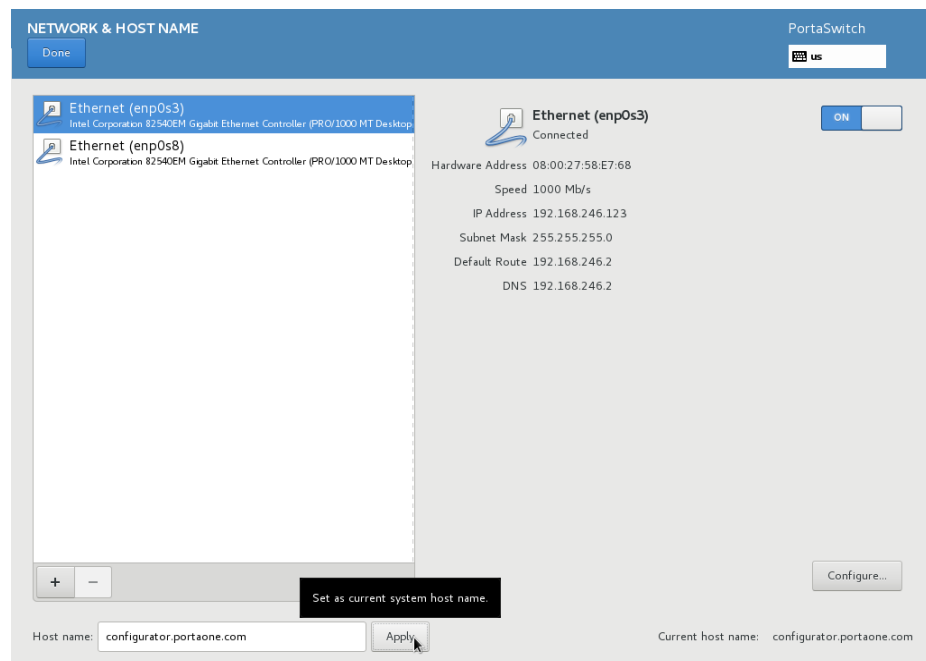


12. Make sure that this network is enabled and that the corresponding
    switch button is set to "ON."
13. If the server also requires a public IP address, choose the network
    interface that is connected to a *public LAN segment* and repeat steps

**24**

4–11 (specifying network details that will be used for external communication for steps 5–6).

14. Click **Done**.

> **NOTE:** Make sure that the **Automatically connect to this network when available** checkbox is selected for both networks.

# Step 9: Begin installation

On the **Installation summary** page, click the **Begin Installation** button. The installation process will redirect you to the **Configuration** page.

This page presents two sections that deal with user settings: **Root Password** and **User Creation**. It is necessary to complete the **Root Password** section during the installation.

It is not recommended that you create server users during the PortaSwitch® installation. The preferred method is to skip the user creation step at this time and create the users later via the Configuration server web interface. This will provide you with a set of instruments that allows you to manage your system users in a much more convenient manner.
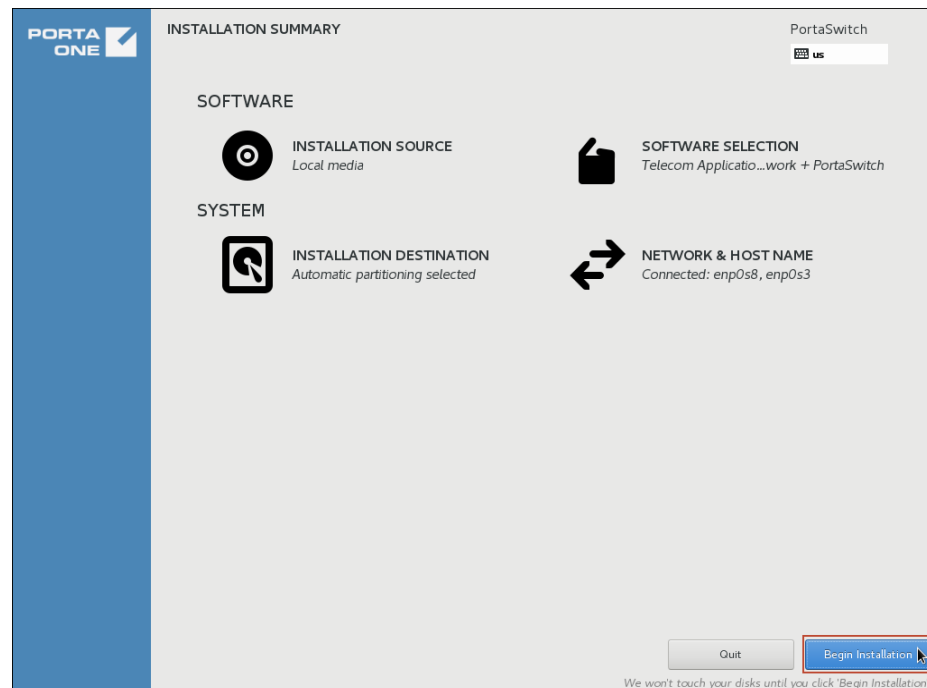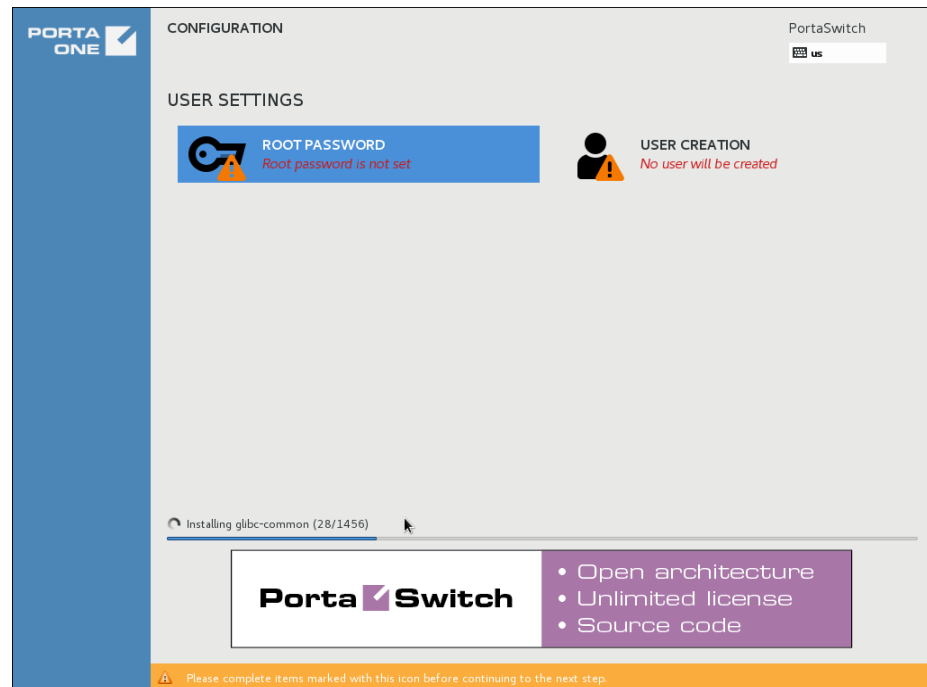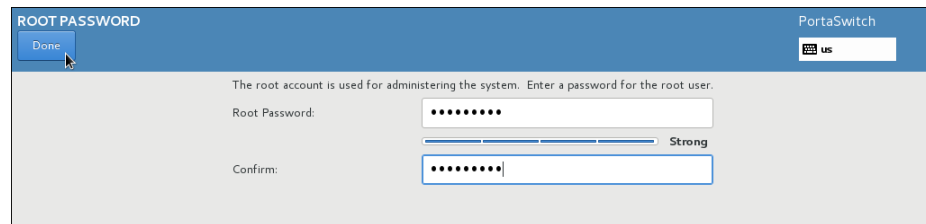
# Step 10: Root password

Choosing the super user password is very important, as you will need it to perform system administration or system recovery.
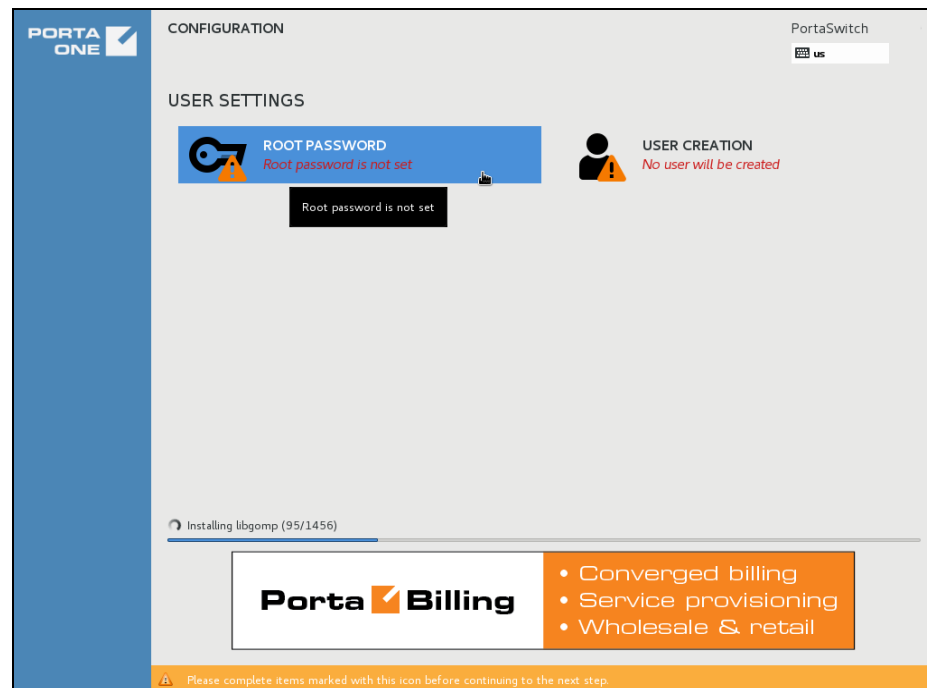
1. On the **Configuration** page, choose **Root Password**.
2. Enter a password for the root user.
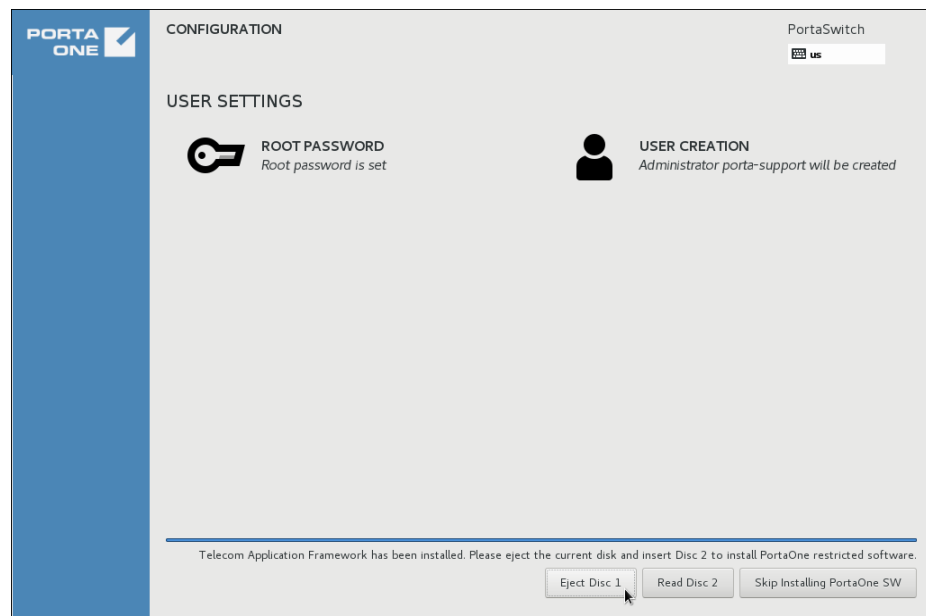
   **NOTE:** Choose a password which will be difficult to guess or crack. A good password is at least 8 characters long, includes numbers, upper and lower case letters and punctuation.

3. Confirm the password.
4. Click **Done**.

Keep this password secure and do not send it via email to the PortaOne support team – they have their own credentials to access your server for doing the post-installation tasks.

# Step 11: Change installation medium

During the installation you will be prompted to insert the second installation medium.



To proceed with the installation:
1. Click **Eject Disc 1**.

2. Insert the installation medium (optical disc or USB flash drive) with PortaSwitch® installation Disc 2 into the computer, and click **Read Disc 2**.

**NOTE:** In rare cases, a server may not detect the second installation USB flash drive. If you experience this issue, please contact our support team, and our support engineers will help you to proceed with the installation.

# Step 12: Reboot

When the installation has finished, the following "Complete!" message appears at the bottom of the page:
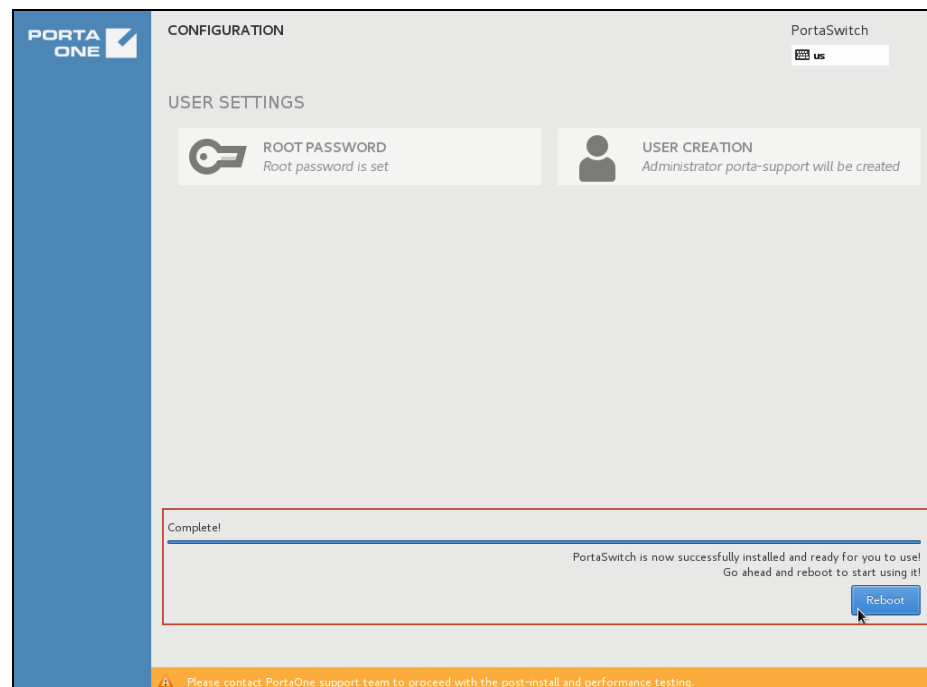


Now you need to reboot the system.
1. Eject the installation medium (optical disc / USB flash drive) from the computer.
2. Click **Reboot**.

Do not forget to enter BIOS again and change the priority of the boot devices so that the hard drive will be attempted first. (This ensures a quicker reboot when recycling the server.)

# Step 13: Hardware check

Next, the installation process will check your server's hardware components, such as CPU, memory and HDDs.

**NOTE**: This step must be executed (HDD speed test done) and the **Suitability Checker** application must be closed before proceeding to the next steps.

```
Suitability Checker
------------------
                    ┤ Suitability Checker ├
    │
    │    Welcome to PortaOne Suitability Checker.
    │
    │    The server meets the requirements for installing MR50-0 PortaOne
    │    products.
    │
    │    CPU(s):   SUBOPTIMAL - 2CPUs with 2 cores were found.
    │    RAM:            OK - 32768 MB
    │    HDD(s):         OK - sda (992492 MB)
    │    NIC(s):         OK - eth0 eth1
    │    USB(s):         OK -
    │
    │
    │
    │    -------------------------------------------------------------
    │
    │               <Test HDD Speed>    <Cancel>
    │
```
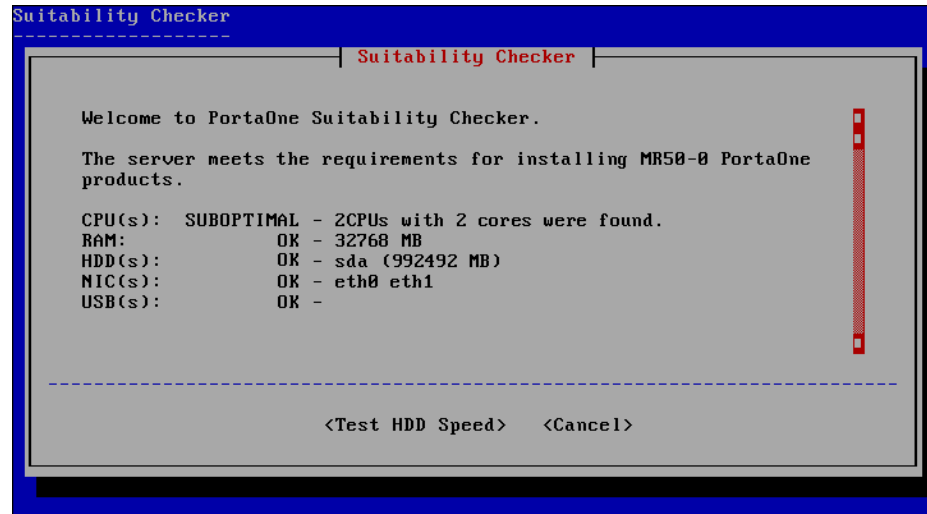
Fast disk read / write speed is crucial for most of the PortaSwitch servers, especially those that run database applications. Execute **Test HDD Speed** to verify that the system provides a sufficient level of performance and that there are no bottlenecks (e.g. caused by a RAID misconfiguration).

# Step 14: Check if system can reboot to normal state

It is good to make sure that the system is in a stable state, and that it returns to normal operations without intervention on reboot, especially if there is no keyboard or other peripheral attached. Following a normal reboot, the screen should look like this:

```
PortaOne Linux 70.0
Kernel 3.10.0-862.el7.x86_64 on an x86_64

configurator login: _
```
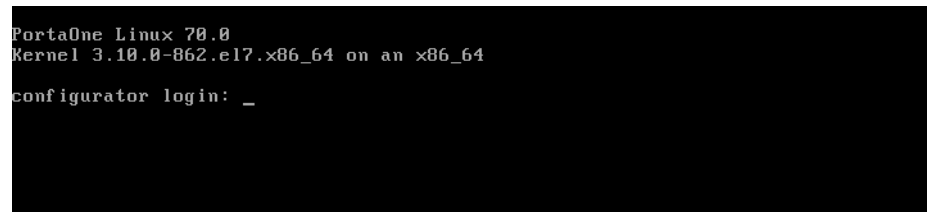
# Step 15: Prepare the system for transportation (optional)

If you need to transport the system to a different location (e.g. hosting center), or otherwise power down the system safely, proceed as follows:

1. Wait until the system finishes booting.
2. Log in as **root**.
3. Type `poweroff`.
4. Wait until either the system powers down on its own, or the message "The operating system has halted" appears, and then power off the server, if it was not done automatically.

# Step 16: Perform initial configuration of PortaSwitch (when all servers have been installed)

Complete steps 1–15 for each server you want to be a part of your PortaSwitch® configuration. Once you have installed the software on the servers, you have a blank system that can be configured in various ways to meet your business requirements. The first (low-level) part of the configuration is usually done by PortaOne support engineers after performing the post-install procedure. For this, contact the PortaOne support team at **support@portaone.com**, who will provide you with further assistance.

In rare cases you may need to perform the configuration by yourself. In this case activate the Configuration server on the appropriate host as described in the **... activate the configuration server?** section of the **How to...** chapter of this guide. Then you can proceed with the system configuration via the Configuration server web interface (for more details, see the *Initial Configuration of PortaSwitch* handbook in the **Unified PortaSwitch Handbook Collection**).

# 4. How to...

# ... Install PortaSwitch® using USB DVD-ROM?

To start the installation using a USB DVD-ROM, follow the steps below:

1. Make sure that all internal optical devices are physically disconnected.
2. In the BIOS setup make sure that USB DVD-ROM is first in the list of boot devices.
3. Insert the first PortaSwitch® installation disc into the USB DVD-ROM and then boot from it.
4. Proceed with the installation by following the instructions in the **Step 3: Starting Installation** chapter of this guide.

# ... Create a bootable USB flash drive from a PortaSwitch® ISO file?

Before starting make sure that you have downloaded both PortaSwitch® ISO installation ISO files and that you have two working USB flash drives at your disposal.

## Create a bootable USB drive in the Linux command-line interface

**Note:** This will erase all information that you currently have on your USB flash drive.

To make PortaSwitch® installation USB flash drives using the Linux command-line interface complete the following steps:

1. Plug the first USB flash drive into the USB port of your computer.
2. Check what name Linux has assigned to your USB flash drive. To do this execute the following command:

```
dmesg | tail -20
```

and look for the strings that contain titles like "sdX," where X can be any letter, e.g. sdb, sdc. This is your USB flash drive name, so remember it since you will need it for the next step. For example, in the screenshot below, the USB flash drive name is sdb.

```
demo@demo-test:~$ dmesg | tail -20
[  905.948241] usb 1-2: Parent hub missing LPM exit latency info.  Power managem
ent will be impacted.
[  905.974286] usb 1-2: New USB device found, idVendor=154b, idProduct=0095
[  905.974290] usb 1-2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[  905.974293] usb 1-2: Product: USB 3.0 FD
[  905.974294] usb 1-2: Manufacturer: PNY Technologies
[  905.974296] usb 1-2: SerialNumber: 1786633642
[  906.070123] usb-storage 1-2:1.0: USB Mass Storage device detected
[  906.072446] scsi3 : usb-storage 1-2:1.0
[  906.072557] usbcore: registered new interface driver usb-storage
[  907.102237] scsi 3:0:0:0: Direct-Access     PNY      USB 3.0 FD       1.00 PQ
: 0 ANSI: 6
[  907.105271] sd 3:0:0:0: Attached scsi generic sg2 type 0
[  907.120131] sd 3:0:0:0: [sdb] 62411243 512-byte logical blocks: (31.9 GB/29.7
 GiB)
[  907.130559] sd 3:0:0:0: [sdb] Write Protect is off
[  907.130564] sd 3:0:0:0: [sdb] Mode Sense: 23 00 00 00
[  907.140278] sd 3:0:0:0: [sdb] Write cache: disabled, read cache: disabled, do
esn't support DPO or FUA
[  907.429208]  sdb: unknown partition table
[  907.486183] sd 3:0:0:0: [sdb] Attached SCSI removable disk
[  908.920576] ISO 9660 Extensions: Microsoft Joliet Level 3
[  908.939550] ISO 9660 Extensions: RRIP_1991A
[  909.483213] systemd-hostnamed[2363]: Warning: nss-myhostname is not installed
```

3. Write the first PortaSwitch® installation ISO file to the USB flash drive. To do this, execute the following command (replace `/Dir1/PortaSwitch_installation_file1.iso` with the path to the first PortaSwitch® installation ISO file and `sdX` with your USB flash drive name):

```
sudo dd if=/Dir1/PortaSwitch_installation_file1.iso
of=/dev/sdX bs=8M
```

```
demo@demo-test:~$ sudo dd if=~/Downloads/PortaSwitch-MR50.0-asm-2-20150909-Porta
One-disc1.iso of=/dev/sdb bs=8M
[sudo] password for demo:
```

4. After the writing process finishes, unplug the first USB flash drive and plug in the second one.
5. Write the second PortaSwitch® installation ISO file on this USB flash drive. To do this repeat steps 2 and 3, but in step 3, specify the name of the second PortaSwitch® installation ISO file.

## Create a bootable USB drive in Windows

There are a lot of programs for Windows that help create bootable USB flash drives and you can use any one that you like. Here we use ROSA Image Writer for the purpose of demonstration.

**Note:** This will erase all information that you currently have on your USB flash drive.

1. Download ROSA Image Writer and open it.
2. Plug the first USB flash drive into the USB port of your computer.

3. Click the ![Open image file icon] **Open image file** button, and select the first PortaSwitch® installation ISO file.
4. From the **USB Device** menu, select the USB flash drive which you want to use. If the drive does not appear in the list, make sure it is plugged into the USB port on your PC, click ![Refresh icon] **Refresh the list**.
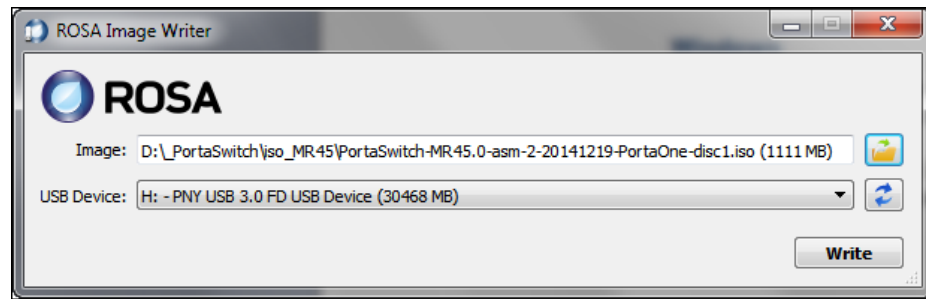5. Click **Write**.
6. After the program informs you that writing process has finished, click **OK**, unplug the first USB flash drive, and plug in the second one.
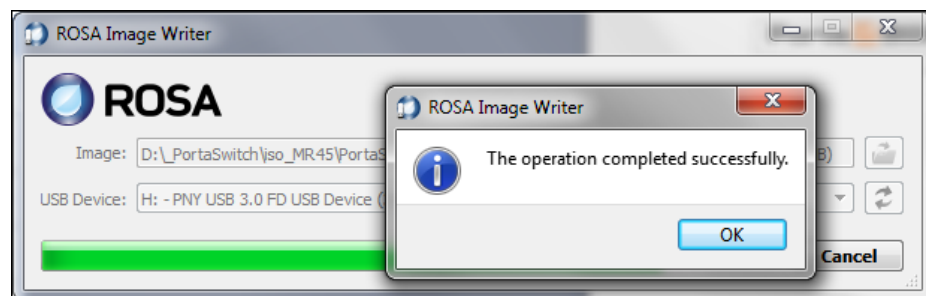


7. Write the second PortaSwitch® installation ISO file on this USB flash drive. To do this repeat steps 3–5, but select the second PortaSwitch® installation ISO file in step 3.

# ... Perform basic troubleshooting?

If the installation process doesn't seem to be proceeding normally, reboot your system and choose the **Troubleshooting** option on the **Installation Menu** page.

34
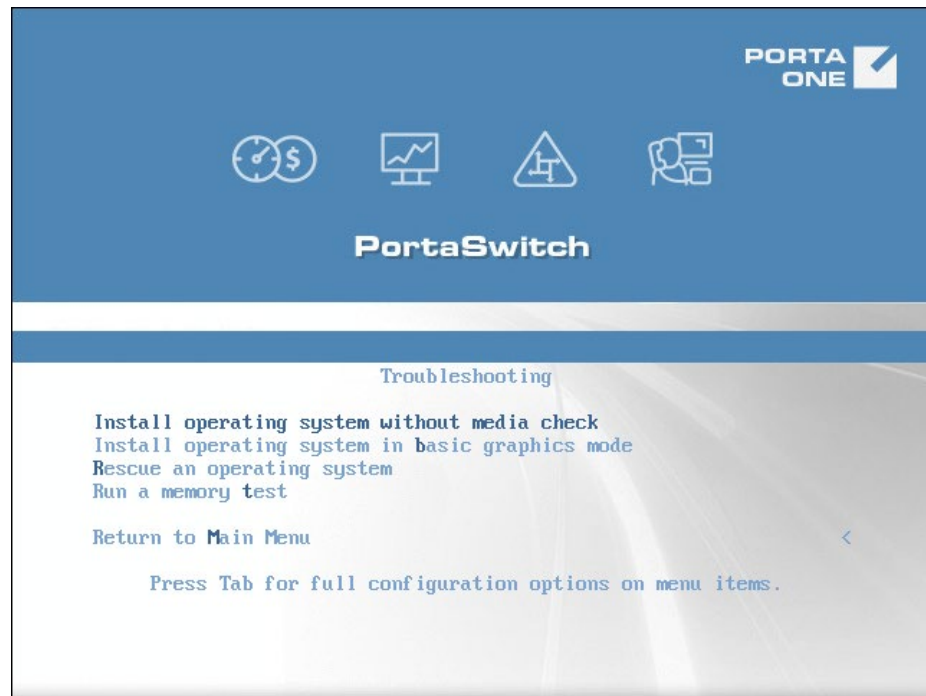
Or, for UEFI:
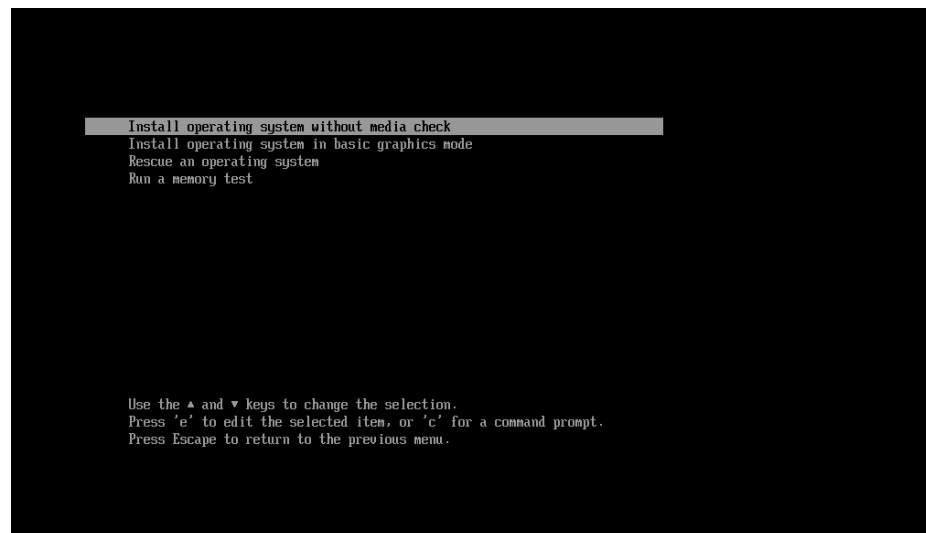


The following troubleshooting tools are available:

- **Install operating system without media check.** The installation utility won't check the installation medium for integrity prior to proceeding with the installation process. This option can be useful, for example, if you have an old disc and the media check that runs by default takes too long.
- **Install operating system in the basic graphics mode.** If after you started the installation process your screen looks distorted or you can't see anything at all, it may be the result of problems with

video drivers. In that case, reboot your system and choose this installation method.

- **Rescue an operating system.** This option calls a command-line environment. Use it if your system doesn't boot and you need to access your files to repair your system.
- **Run a memory test.** Some system issues may be caused by memory problems. Run this utility to check if the RAM is working correctly.

The last two options can be run outside of the installation process.

You can view and configure boot option in the command line that becomes available when you choose an installation option and press **Tab** (or the **E** key, if you use UEFI**)**. For additional information about boot options refer to the **Oracle Linux documentation**.

# ... Activate the configuration server?

This is usually done by PortaOne Support engineers after performing the post-install procedure. But if for some reason you need to activate the Configuration server right after the installation, you can use the following script:

```
/home/porta-configurator/utils/porta-configurator-install.sh
```

- Use -h option to get help on script usage:

```
/home/porta-configurator/utils/porta-configurator-install.sh -h
```

- Use -b option to activate the Configuration server with the default parameters (without additional prompts):

```
/home/porta-configurator/utils/porta-configurator-install.sh -b
```

# 5. Frequently asked questions

# What is the recommended setup for the PortaSwitch® behind a firewall?

Although PortaSwitch® servers are based on the Oracle Linux OS which is designed for high security, it is still reasonable to consider external firewall for better system protection. If you want to position servers *behind* the firewall for some reason (e.g. your corporate network security policy demands this) follow the recommendations below.

## General configuration advice

- We suggest positioning all PortaSwitch® servers into a dedicated network segment.
- Interaction between PortaSwitch® servers via a private network interface must *not* be blocked by a firewall.
- Whatever configuration your private LAN segment has, internal communication between servers (via TCP port 22, etc.) *must* always be granted.
- Do not configure a firewall between nodes of the cluster (i.e. PortaSIP cluster®, etc.).
- For PortaSwitch® sites that span across geographically dispersed locations, all PortaSwitch® servers must be connected via virtual (or physical) Layer 2 connection(s) and all PortaSwitch® servers should be configured as hosts within a single virtual (or physical) private network.

## Ports to be opened

Logical components (e.g. Admin, Billing, Master DB, Replica DB, PortaSIP®) are installed and operating on some hosts. This requires particular ports to be kept open on these hosts, depending on which components are running on each of them. To find out which open ports are required by each component, see the table below:

| Ports to be opened | Description |
|---|---|
| *All servers:* **public interface** | |
| TCP 22 | This is used for server administration via SSH. |
| *Configuration server:* **private interface** | |
| TCP / UDP 5667 5668 | This is required for NSCA to collect monitoring statistics from the servers and send them to the Configuration server in passive mode. |
| TCP 80 | This is used for downloading custom patches during the update process and must be kept open permanently. |
| *Configuration server:* **public interface** | |
| TCP 8700 | This is required for accessing the monitoring system web interface. |
| *Web (admin) server:* **public interface** | |
| TCP 25 | This is used for uploading tariffs via email. |
| TCP 80 | This is used for UA provisioning. |
| UDP 69 | This is required by the TFTP service. |
| TCP 443 | This is required for access to the admin interface. |
| TCP 8442<br>TCP 8443<br>TCP 8444<br>TCP 8445<br>TCP 8446<br>TCP 8447<br>TCP 8448 | This is required for access to the self-care web interfaces:<br><br>Reseller self-care<br>PortaSIP XML / JSON API<br>Customer self-care, distributor self-care<br>Account self-care<br>Reseller's helpdesk<br>Vendor self-care<br>Representative self-care |
| TCP 8449 | This is required for access to the WiMax session status page. |
| TCP 8600<br>TCP 8601 | This is required for access to web signup pages:<br><br>Web signup<br>Multicard web signup |
| TCP 8901<br>TCP 8903-8904 | This is required to access callback services:<br><br>Web callback<br>SMS callback |
| TCP 8943 | This is used to access webmail. |

| Ports to be opened | Description |
|---|---|
| *RADIUS (billing) server:* **public interface** | |
| <br><br><br><br><br>UDP 1812<br>UDP 1813 | This is used to serve RADIUS requests from RADIUS clients, such as PortaSIP nodes and web server (required for the Test DialPlan feature):<br><br>RADIUS authentication<br>RADIUS accounting |
| TCP 3868 | This is used to serve DIAMETER requests (optional). |
| UDP 5060 | This is used to accept SIP requests and responses from the SIP nodes. |
| *PortaSIP® dispatching SBC:* **public interface** | |
| UDP 5060 | This is used to accept SIP requests and responses from the SIP nodes. |
| TCP 5061 | This is required for SIP over TCP support |
| TCP 5051 | This is required for SIP over TLS support. Disabled by default. |
| *PortaSIP® dispatching node:* **virtual IP address** | |
| UDP 5060 | This is used to accept SIP requests and responses from the SIP nodes. |
| TCP 5060 | This is required for SIP over TCP support. |
| UDP 5070 | This is used by Limit Controller to accept SIP requests and responses from the SIP nodes |
| TCP (TLS) 5051 | This is required for SIP over TLS support. Disabled by default. |
| SMPP 2775 | This is required to accept and send SMPP messages. |
| TCP 8101 | This is required for the SMTP transport. |
| TCP 8081 | This is required for the IMAP transport. |
| TCP 8091 | This is required for the IMAPS transport. |
| *PortaSIP® processing node:* **public interface** | |
| UDP 35000–65000 | This is used for RTP proxying. |
| *MySQL (Master DB, Replica DB) servers:* **can be configured to use either private or public interfaces** | |
| <br><br><br>TCP 3306<br>TCP 3307 | This is used to serve database requests from the billing server, web server and PortaSIP® servers:<br>MainDB server<br>ReplicaDB server |

| Ports to be opened | Description |
|---|---|
| *Oracle DB servers:* **can be configured to use either private or public interfaces** | |
| TCP 9521 | This is used to serve database requests from the billing server, web server and PortaSIP® servers. |
| TCP 1158 | This is used for Oracle Enterprise Manager access. |

| Ports to be opened | Description |
|---|---|
| *All servers:* **public interface** | |
| TCP 22 | This is used for server administration via SSH. |
| *Configuration server:* **private interface** | |
| TCP / UDP 5667 5668 | This is required for NSCA to collect monitoring statistics from the servers and send them to the Configuration server in passive mode. |
| TCP 80 | This is used for downloading custom patches during the update process and must be kept open permanently. |
| *Configuration server:* **public interface** | |
| TCP 8700 | This is required for accessing the monitoring system web interface. |
| *Web (admin) server:* **public interface** | |
| TCP 25 | This is used for uploading tariffs via email. |
| TCP 80 | This is used for UA provisioning. |
| UDP 69 | This is required by the TFTP service. |
| TCP 443 | This is required for access to the admin interface. |
| TCP 8442<br>TCP 8443<br>TCP 8444<br>TCP 8445<br>TCP 8446<br>TCP 8447<br>TCP 8448 | This is required for access to the self-care web interfaces:<br><br>Reseller self-care<br>PortaSIP XML / JSON API<br>Customer self-care, distributor self-care<br>Account self-care<br>Reseller's helpdesk<br>Vendor self-care<br>Representative self-care |
| TCP 8449 | This is required for access to the WiMax session status page. |
| TCP 8600<br>TCP 8601 | This is required for access to web signup pages:<br><br>Web signup<br>Multicard web signup |

| Ports to be opened | Description |
|---|---|
| TCP 8901<br>TCP 8903-8904 | This is required to access callback services:<br><br>Web callback<br>SMS callback |
| TCP 8943 | This is used to access webmail. |
| *Web (admin) server:* **private interface** | |
| UDP 5405 | This is used by the corosync service for internal communication among cluster nodes. Must be opened if you deploy web cluster. |
| *OCS server:* **public interface** | |
| UDP 1812<br>UDP 1813 | This is used to serve RADIUS requests from RADIUS clients, such as PortaSIP nodes and web server (required for the Test DialPlan feature):<br><br>RADIUS authentication<br>RADIUS accounting |
| TCP 3868 | This is used to serve DIAMETER requests (optional). |
| UDP 5060 | This is used to accept SIP requests and responses from the SIP nodes. |
| *OCS server:* **private interface** | |
| UDP 5405 | This is used by the corosync service for internal communication among cluster nodes. Must be opened if you deploy Diameter cluster. |
| *PortaSIP® dispatching SBC:* **public interface** | |
| UDP 5060 | This is used to accept SIP requests and responses from the SIP nodes. |
| TCP 5061 | This is required for SIP over TCP support |
| TCP 5051 | This is required for SIP over TLS support. Disabled by default. |
| TCP 9442<br>TCP 9443<br>TCP 9444<br>TCP 9445<br>TCP 9446<br>TCP 9447<br>TCP 9448<br>TCP 9449 | This is required for dual-version PortaSwitch deployment to access the self-care web interfaces:<br><br>Reseller self-care<br>Administrator self-care<br>Customer self-care, distributor self-care<br>Account self-care<br>Reseller's helpdesk<br>Vendor self-care<br>Representative self-care<br>Session status interface |

| Ports to be opened | Description |
|---|---|
| TCP 9600<br>TCP 9601 | This is required for dual-version PortaSwitch deployment to access web signup pages:<br><br>Web signup<br>Multicard web signup |
| *PortaSIP® dispatching node:* **virtual IP address** | |
| UDP 5060 | This is used to accept SIP requests and responses from the SIP nodes. |
| TCP 5060 | This is required for SIP over TCP support. |
| TCP (TLS) 5051 | This is required for SIP over TLS support. Disabled by default. |
| SMPP 2775 | This is required to accept and send SMPP messages. |
| TCP 8101 | This is required for the SMTP transport. |
| TCP 8081 | This is required for the IMAP transport. |
| TCP 8091 | This is required for the IMAPS transport. |
| *PortaSIP® dispatching node:* **private interface** | |
| UDP 5405 | This is used by the corosync service for internal communication among cluster nodes. |
| *PortaSIP® processing node:* **public interface** | |
| UDP 35000–65000 | This is used for RTP proxying. |
| *MySQL (Master DB, Replica DB) servers:*<br>**can be configured to use either private or public interfaces** | |
| TCP 3306<br>TCP 3307 | This is used to serve database requests from the billing server, web server and PortaSIP® servers:<br>MainDB server<br>ReplicaDB server |
| *Oracle DB servers:*<br>**can be configured to use either private or public interfaces** | |
| TCP 9521 | This is used to serve database requests from the billing server, web server and PortaSIP® servers. |
| TCP 1158 | This is used for Oracle Enterprise Manager access. |

Please note that this list may be extended in the future.

## Outgoing connections

All servers must be granted permanent access to the following PortaOne servers in order to ensure that services function correctly:

| Server | Protocol | Port |
|---|---|---|
| license1.portaone.com | TCP | 80 |
| license2.portaone.com | TCP | 80 |

For your servers' health monitoring purposes, the Configuration server must be granted access to the PortaOne monitoring servers:

| Server | Protocol | Port |
|---|---|---|
| monitor1.portaone.com | TCP / UDP | 5667, 5668 |
| monitor2.portaone.com | TCP / UDP | 5667, 5668 |

For performing updates to newer releases and for troubleshooting purposes, all servers must be granted access to:

| Server | Protocol | Port |
|---|---|---|
| packages.portaone.com | TCP | 80, 443 |
| git.portaone.com | TCP | 29418 |

In order to automatically submit call logs to PortaOne's support ticketing system grant access from your web server to the following:

| Server | Protocol | Port |
|---|---|---|
| smtp-in.portaone.com (MX record for portaone.com) | TCP | 25 |

Make sure that your servers are able to connect to any server from the pool of time servers for time synchronization. You can find the list of NTP pool time servers on the NTP site:

**http://support.ntp.org/bin/view/Servers/NTPPoolServers**

**NOTE:** All PortaSwitch® servers can receive time information and synchronize that with the Configuration server and the PortaSIP® server.

Port should be opened for NTP service on all servers of the installation

| Server | Protocol | Port |
|---|---|---|
| Any server from the pool of time servers for time synchronization | UDP | 123 |

If you wish to use your own NTP server, please notify us and we'll adjust the configuration of the NTP service.

The Geo-IP database in your installation is regularly updated to ensure that the Geo-IP Fraud Prevention feature works correctly. Allow your RADIUS servers to establish connections to the MaxMind's downloadable databases (updates.maxmind.com) via HTTP / HTTPS

protocol. If you are running a firewall, geo-update requires that the DNS and HTTPS (443) ports be open.

## Incoming connections

For troubleshooting purposes, allow incoming connections to your servers from the following PortaOne IP addresses:

- 217.182.15.211
- 217.182.15.212
- 217.182.15.213
- 217.182.15.214
- 217.182.15.215
- 217.182.15.216
- 217.182.15.217
- 34.209.225.48
- 52.209.93.49
- 66.70.164.127
- 66.70.164.128
- 193.28.87.55
- 193.28.87.93
- 193.28.87.22
- 193.28.87.62
- 91.212.34.4
- 193.34.92.88
- 193.34.92.224