One Identity Safeguard for Privileged Sessions 6.9.5

Deployment on Amazon Web Services

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

SPSDeployment on Amazon Web Services
Updated - 08 March 2023, 10:05

For the most recent documents and product information, see Online product documentation.

Contents

Introduction **4**

Prerequisites **5**

Limitations **6**

Installing SPS on Amazon Web Services **7**

About us **19**

Contacting us **20**

Technical support resources **21**

1

Introduction

The aim of this guide is to provide detailed, step-by-step instructions on how to set up and install One Identity Safeguard for Privileged Sessions in an Amazon Web Services (AWS) virtual environment.

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. Please consult One Identity's Product Support Policies for more information on environment virtualization.

The document comprises the following sections:

- Prerequisites collects the requirements that you must comply with before deploying SPS on AWS.
- Limitations lists the limitations that apply when installing SPS in an AWS virtual environment.
- Installing SPS on Amazon Web Services describes how to install SPS in an AWS virtual environment.

2

Prerequisites

The following prerequisites must be met before deploying SPS on Amazon Web Services:

- You have a valid One Identity Safeguard for Privileged Sessions license.

  One Identity Safeguard for Privileged Sessions uses the "Bring your own license" model. Note that to deploy two active SPS nodes as an availability set, you must purchase two standalone SPS licenses. To purchase a license, contact our Support Team.
- You have an Amazon Web Services account and privileges to access the Amazon Elastic Compute Cloud (EC2) service.
- You have secure access to your Amazon Virtual Private Cloud (VPC) resources, for example, through the use of a Virtual Private Network (VPN).
- You have working knowledge of the SPS installation process.
- You have familiarity with AWS EC2.

3

Limitations

The following limitations apply when deploying SPS on Amazon Web Services:

- If High Availability (HA) operation mode is required in a virtual environment, use the HA function provided by the virtual environment.
- When running SPS in a virtual environment, use a single network interface.
- During AWS installation, connecting directly to the Internet using a public IP address is not supported. Instead, you must access the Internet via a Virtual Private Network or a jump host.

Installing SPS on Amazon Web Services

The following describes how to deploy One Identity Safeguard for Privileged Sessions on Amazon Web Services.

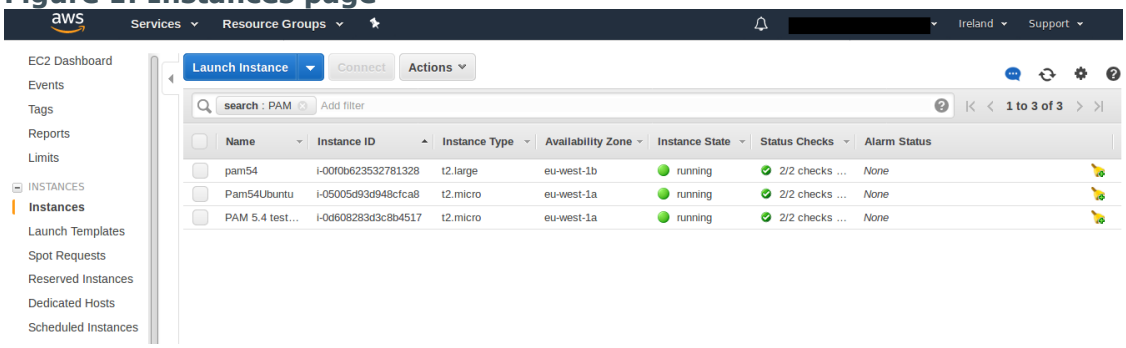
NOTE: This chapter uses a number of screenshots for illustration purposes. Note that these are added here for reference only as the look and feel (but not the contents) of the Amazon user interface may change without this guide showing the latest changes.

To deploy One Identity Safeguard for Privileged Sessions on Amazon Web Services

1. Log in to Amazon Web Services.

   Once logged in, go to **INSTANCES > Instances** in the left-hand navigation pane, and then click **Launch Instance**. Alternatively, from the menu, select **Services > Compute > EC2 > INSTANCES > Instances**.

   Figure 1: Instances page

2. The **Step 1: Choose an Amazon Machine Image (AMI)** page comes up.
3. Choose an AMI that corresponds to the type of Virtual Machine (VM) that you wish to launch an instance from:

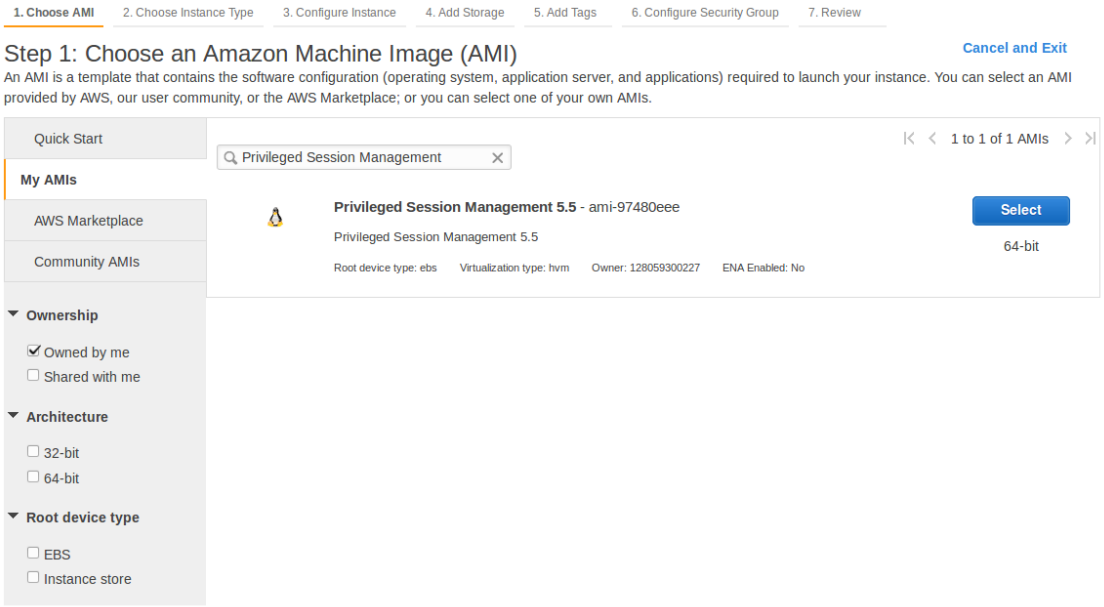
a. Click **My AMIs** in the left-hand navigation pane.

b. Go to **Ownership**, and select the **Shared with me** checkbox. Deselect the **Owned by me** checkbox. This will apply a filter and display the AMIs relevant to you.

c. Click your preferred AMI, and click **Select** next to it.

TIP: To quickly find the AMI you are looking for, type a search keyword in the **Search my AMIs** search box and hit`Enter`.

Figure 2: Step 1: Choose an Amazon Machine Image (AMI)



The **Step 2: Choose an Instance Type** page comes up.

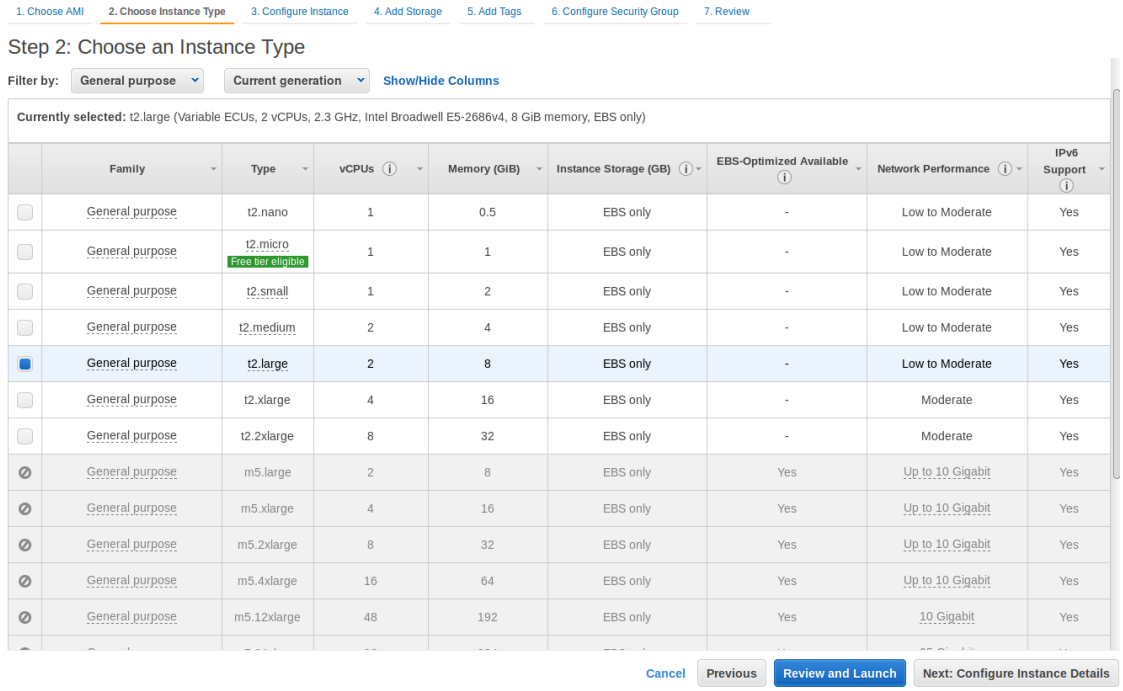
4. Choose an instance type:

   a. Select an instance type by clicking the checkbox next to it.

      NOTE: The minimum memory requirement is 8 GiB, that is, type *t2.large*. For your specific memory requirement, contact Support.

   b. Click**Next: Configure Instance Details**.

Figure 3: Step 2: Choose an Instance Type



The **Step 3: Configure Instance Details** page comes up.

5. Configure instance details:
    a. Select the required Virtual Private Cloud (VPC) from the **Network** list.
    b. Choose a subnet to launch the instance into.

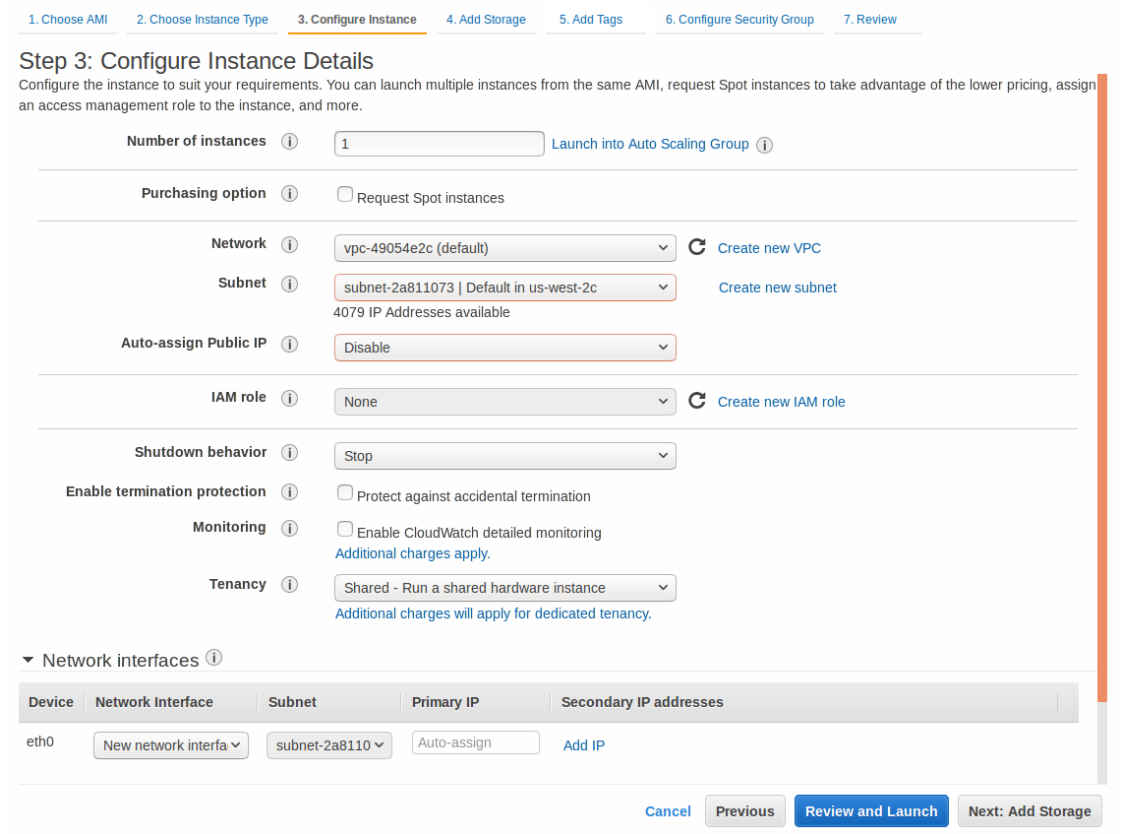
    > NOTE: Exposing SPS to the public Internet during installation is not supported at all, therefore, you must use a VPN or jump host to reach your instance and configure it.

    c. Ensure that the **Auto-assign Public IP** field is set to **Disable** or **Use subnet setting (Disable)**. This is required so that you do not get assigned a public IP address.
    d. Use the default values for all other fields or change them as required.
    e. You can leave the **Network interfaces** part untouched as using just one network interface will suffice.

    Note, however, that if you launch SPS with a single interface configured, then that interface will act as the management interface.

    f. Click**Next: Add Storage**.

Figure 4: Step 3: Configure Instance Details



The **Step 4: Add Storage** page comes up.

6. Add storage to your instance:

   a. Set the size of your instance's store volume.

      NOTE: Choose this value wisely as once you have launched the instance, you will not be able to go back and modify it. The minimum storage size is 20 GiB, while the maximum allowed value is 16 TB (16384 GB).

   b. Set the volume type of your instance's store volume.

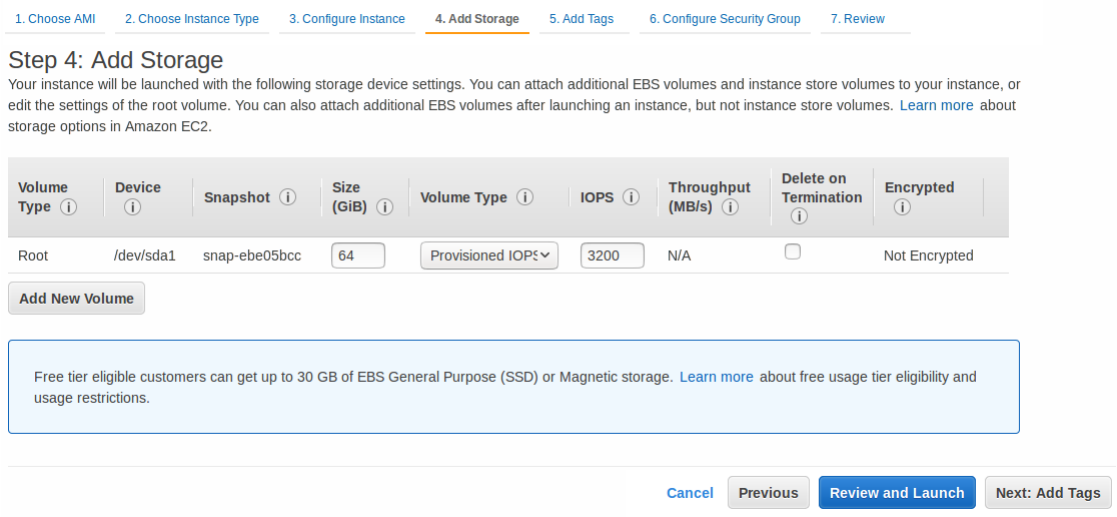
      SSD provides better performance than a Magnetic hard drive, however, it is also more expensive.

      For a customer specific volume type and disc recommendation, contact Support to discuss your needs.

      TIP: Selecting the **Delete on Termination** checkbox will automatically delete your store volume on terminating the instance. This is useful as this will free up storage place, and you will not have to pay for a store volume you are not using anymore. However, note that deleting the store volume will also delete your non-archived audit data.

   c. Click**Next: Add Tags**.

Figure 5: Step 4: Add Storage



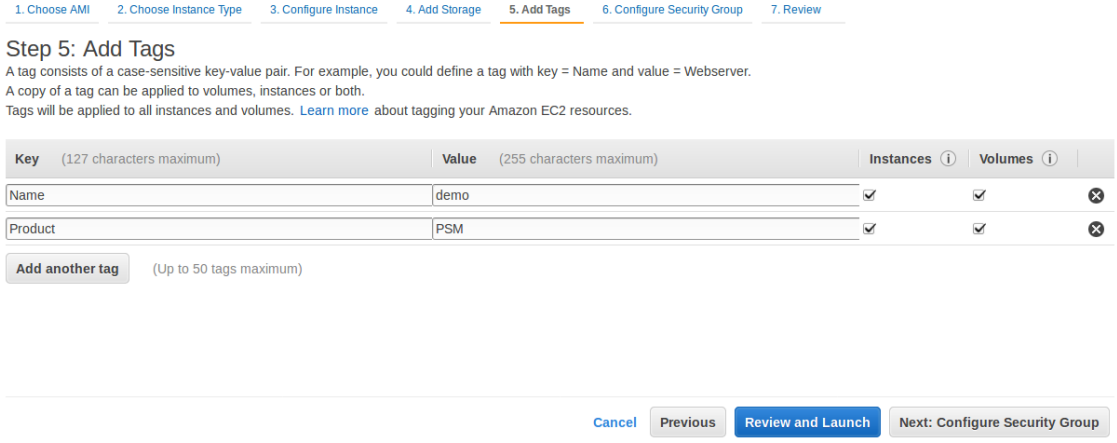
The **Step 5: Add Tag** page comes up.

Create a tag for your instance:

a. Add a meaningful key-value pair that will help you later on to easily identify your instance.

b. Click**Next: Configure Security Group**.

Figure 6: Step 5: Add Tags



7.

The **Step 6: Configure Security Group** page comes up.

8. Configure security group:

a. Set a new or an existing security group to control how SPS is accessed.

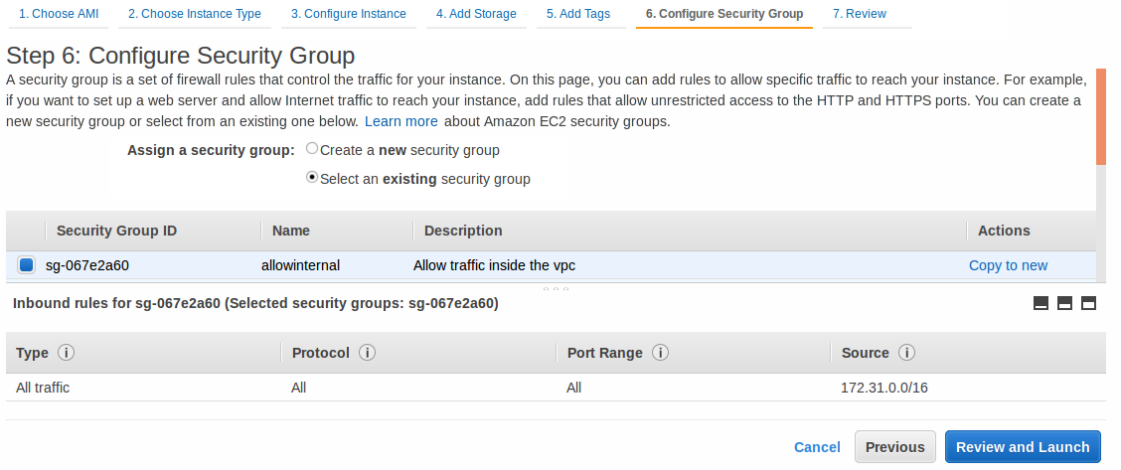
Exposing SPS to the public Internet during installation is not supported at all, therefore, you must use a VPN or jump host to reach your instance and

configure it. As for exposing the logging interface to the Internet after installation, contact Support to discuss your needs and how those could be met.

To achieve the above: restrict your security group to those users and log clients that access SPS from a secure network, and not over the public Internet. For example, if you are using a jump host, then you need a security group that will allow only your dedicated VPC to connect to your SPS. If there is a VPN to your home network or some other secure network, that can be allowed as well.

b. Click **Review and Launch**.

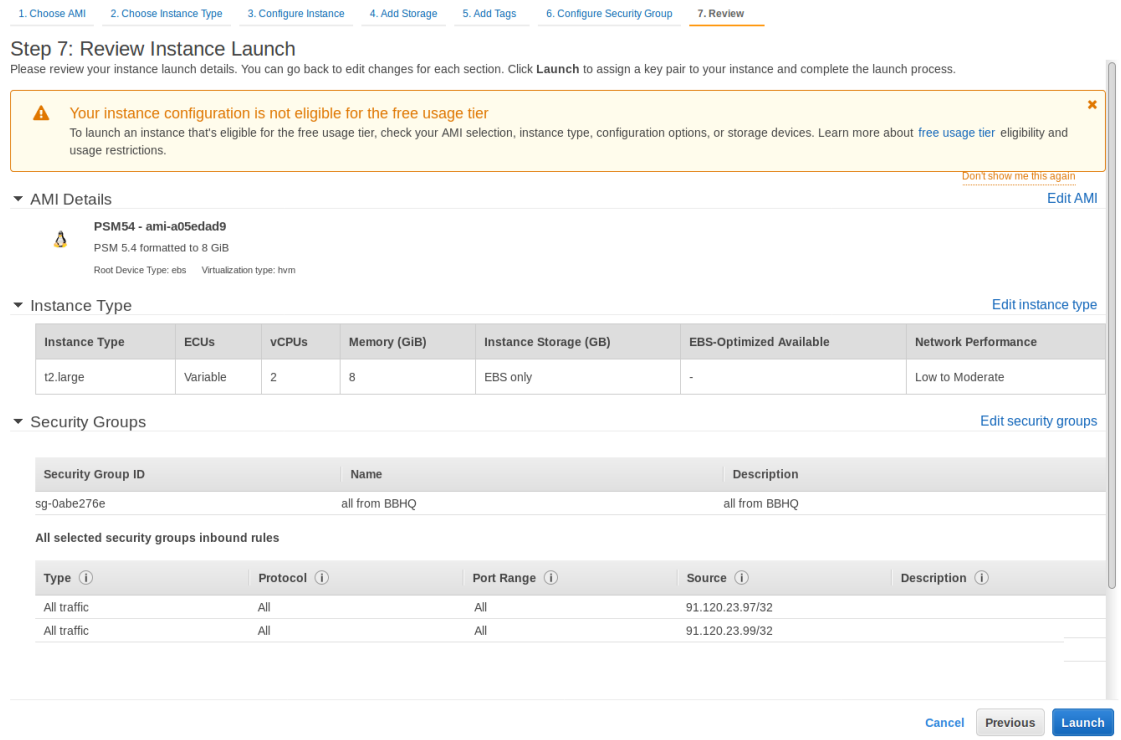
Figure 7: Step 6: Configure Security Group



The **Step 7: Review Instance Launch** page comes up.

9. Before launching your instance, double-check whether all details have been set as intended:
   a. Ensure that:
      - Under **Instance Type**, you have at least 8 GiB of memory assigned.
      - Under **Instance Details**, the **Assign Public IP** option is set to **Disable** or **Use subnet setting (Disable)**.
   b. Make any changes if required.
   c. Once you are happy with all settings, click **Launch**.

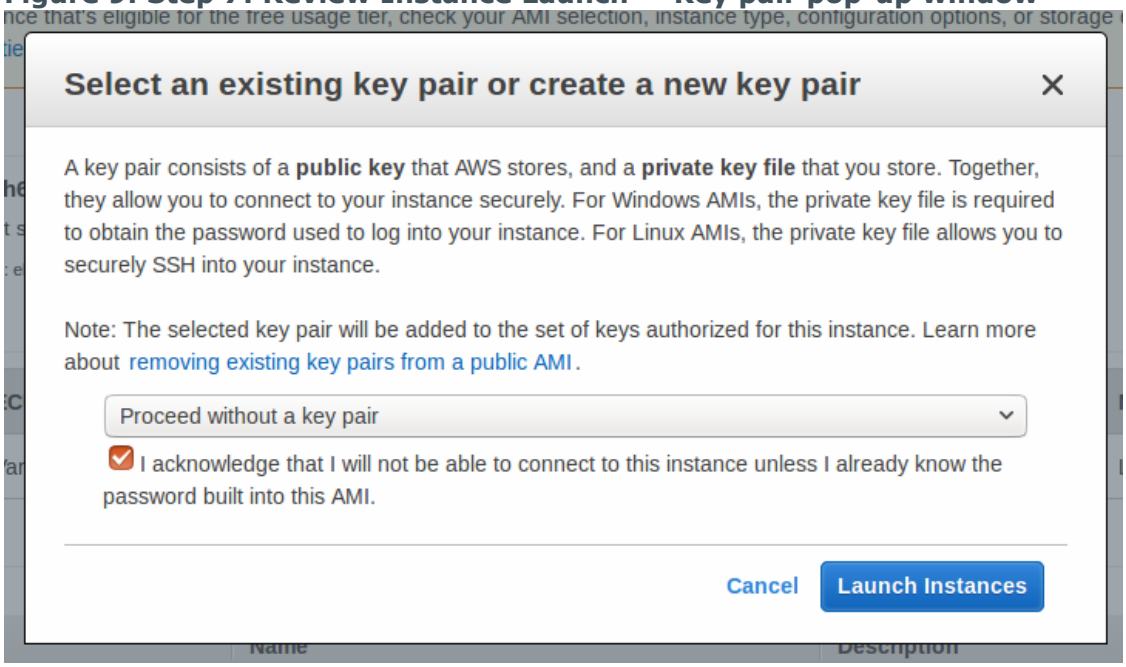
Figure 8: Step 7: Review Instance Launch



The **Select an existing key pair or create a new key pair** pop-up window comes up.

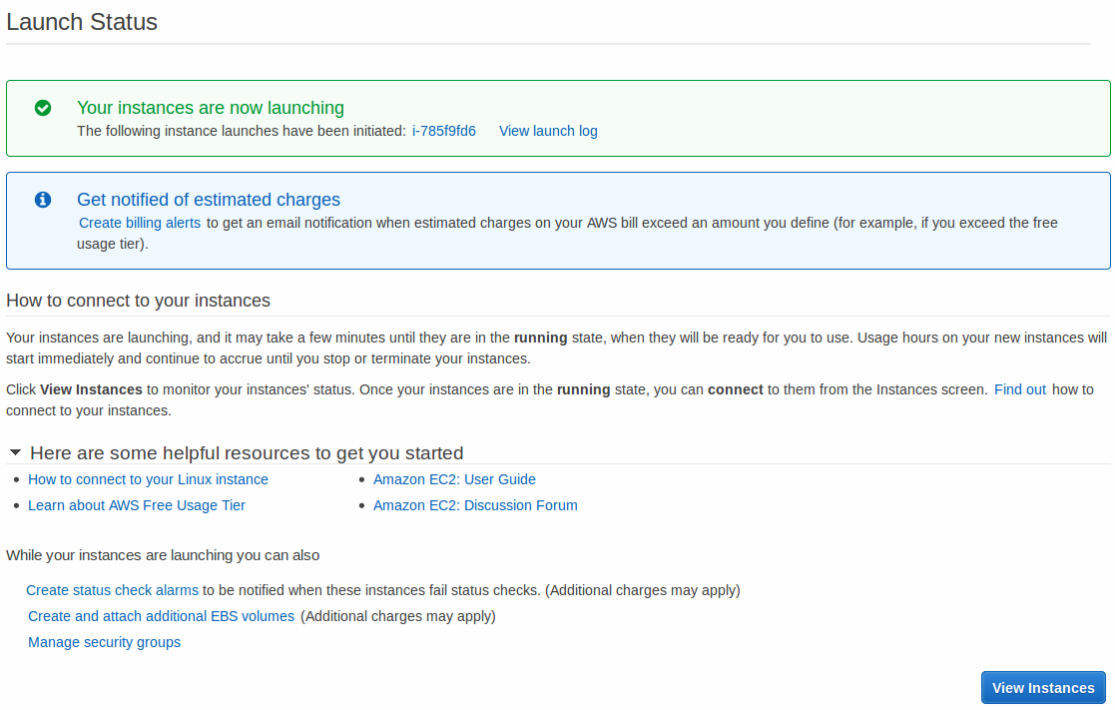
10. On the **Select an existing key pair or create a new key pair** pop-up window:
    a. Select the **Proceed without a key pair** option.
    b. Tick the checkbox that says "I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI".
    c. Click **Launch Instances**.

Figure 9: Step 7: Review Instance Launch — Key pair pop-up window



The **Launch Status** page comes up informing you that your instance is launching. To view your instance's status, click **View Instances**.

Figure 10: Launch Status page



11.

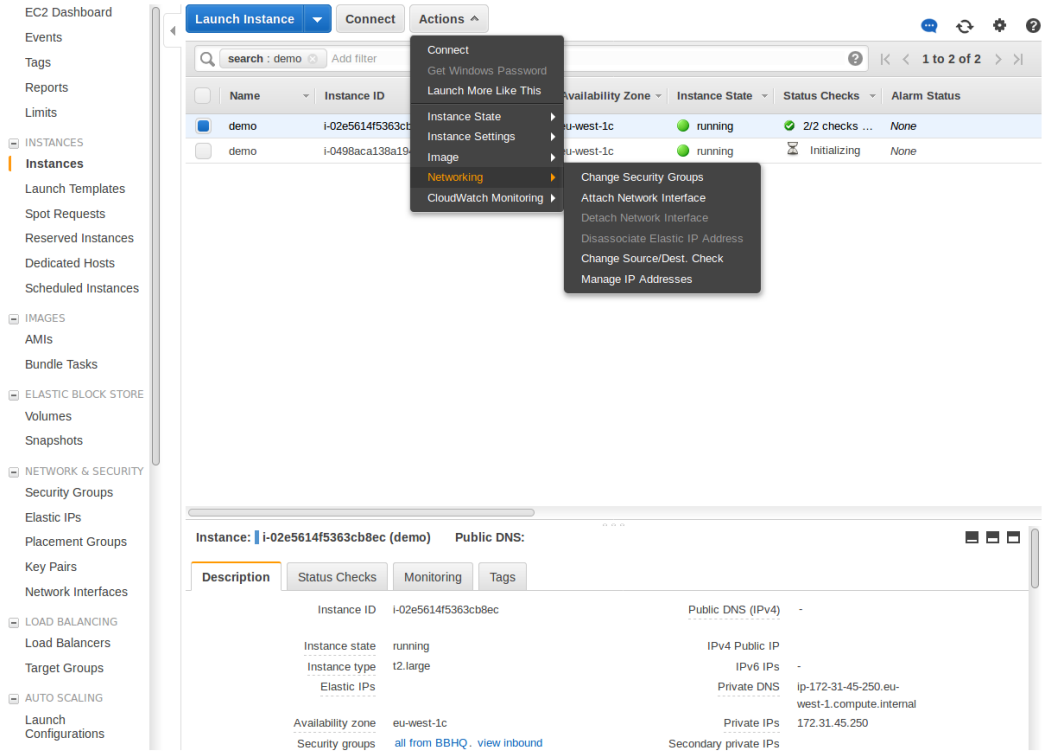
The **Instances** page comes up, which should now display the instance you have just launched. Depending on the size of the instance, installation may take up to 1-5 minutes.

To access your SPS instance and start configuring it using the welcome wizard, you will need your instance's IP address and the netmask of your chosen subnet, both of which you can obtain from the AWS user interface.

12. SPS expects that the IP address provided will not change, therefore, before retrieving the IP address, perform the following check:

    Click the instance you have just added, and select **Actions > Networking > Manage Private IP Addresses** from the menu at the top.

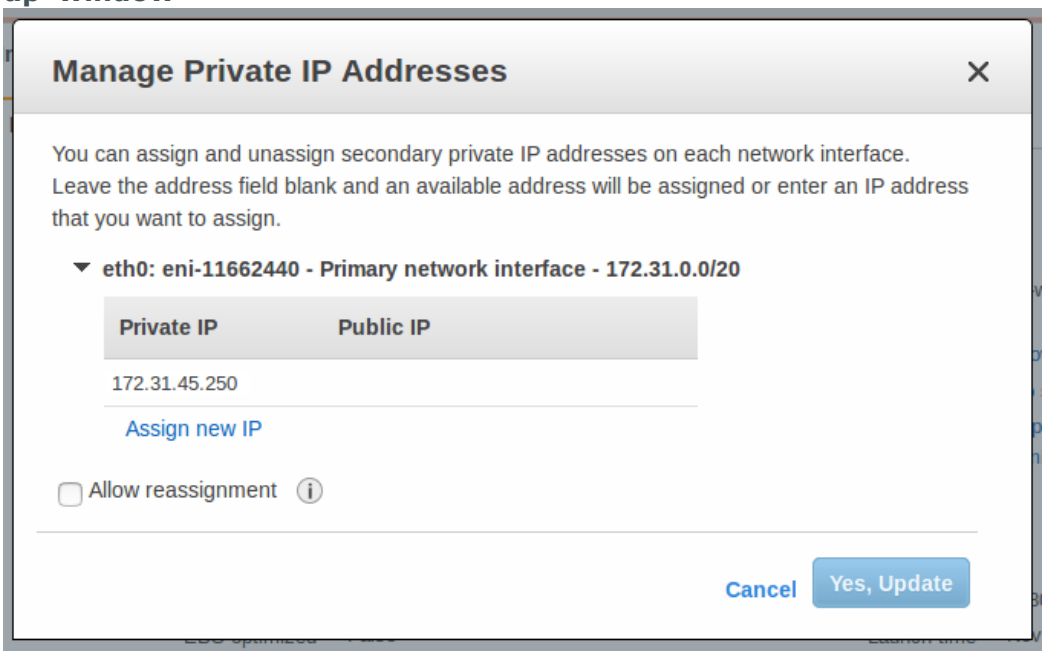
Figure 11: Instances page — Actions menu



a. The **Manage Private IP Addresses** pop-up window comes up.

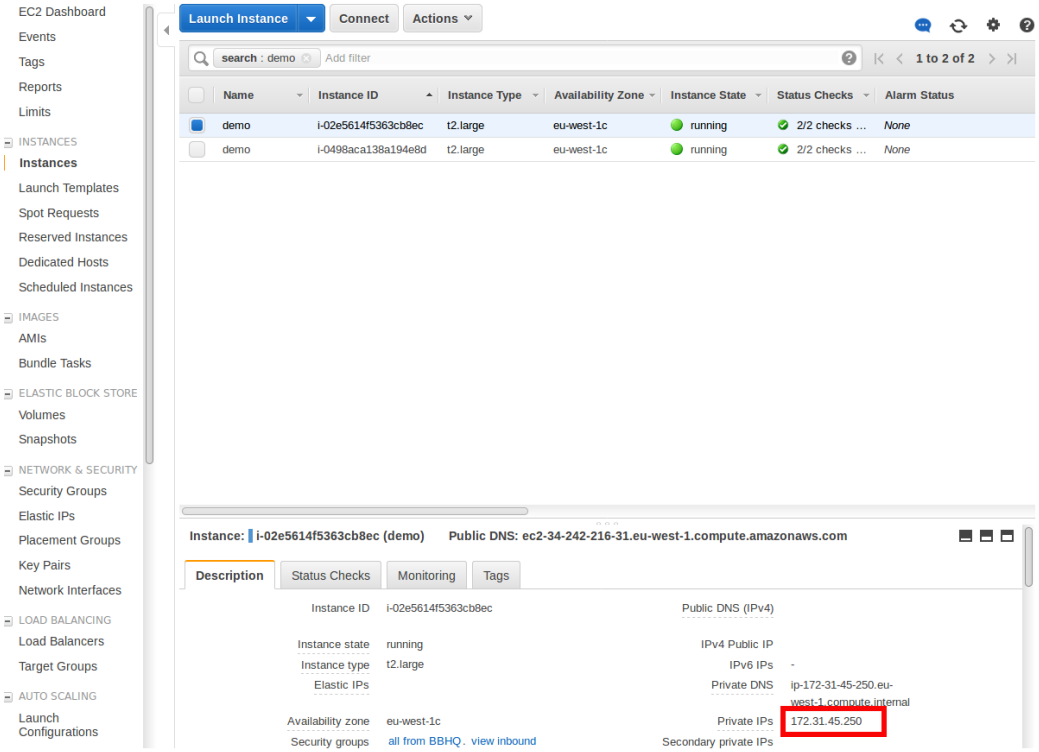
b. To ensure that the IP address stays the same, make sure that the **Allow reassignment** option is unchecked.

Figure 12: Instances page — Manage Private IP Addresses pop-up window



13. To obtain and use the IP address of the instance to access the welcome wizard:
    a. Click the instance on the **Instances** page.
       This will display the description of the instance, including its private IP address.
    b. Select the value in the **Private IPs** field and copy it.

Figure 13: Instances page — Instance description

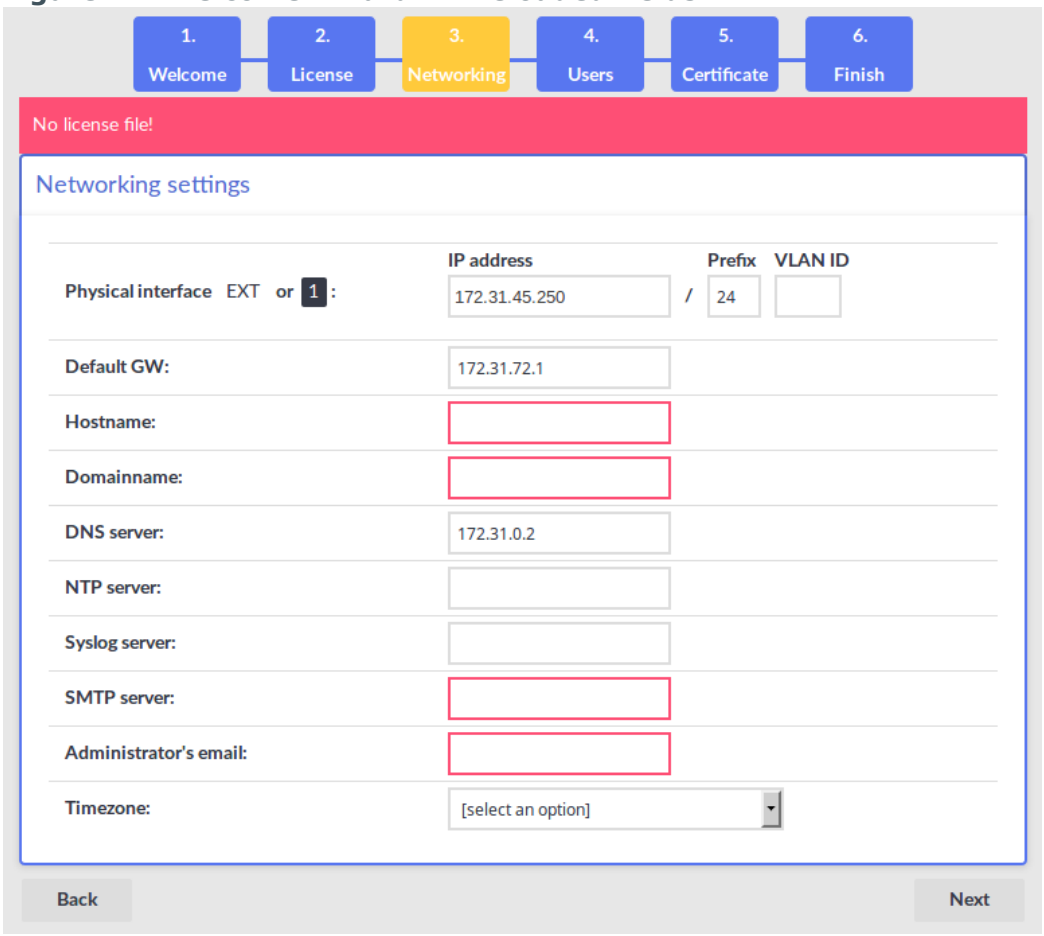


c. Paste the IP you copied in your browser and accept the displayed certificate. The welcome wizard appears.

   The SPS welcome wizard automatically preloads the **IP address**, **Prefix**, **Default GW** and **DNS server** fields as shown in the image below.

   NOTE: If data is not automatically preloaded in your welcome wizard as shown in the image below, contact Support.

Figure 14: Welcome wizard — Preloaded fields



For detailed information on the SPS welcome wizard, see "The Welcome Wizard and the first login" in the Administration Guide.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product