



One Identity Safeguard for Privileged Sessions 6.9.3

Deployment on Amazon Web Services

Copyright 2021 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. 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.

SPS Deployment on Amazon Web Services
Updated - 30 April 2021, 09:20
Version - 6.9.3

Contents

Introduction	4
Prerequisites	5
Limitations	6
Installing SPS on Amazon Web Services	7
About us	19
Contacting us	19
Technical support resources	19

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.

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.

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.

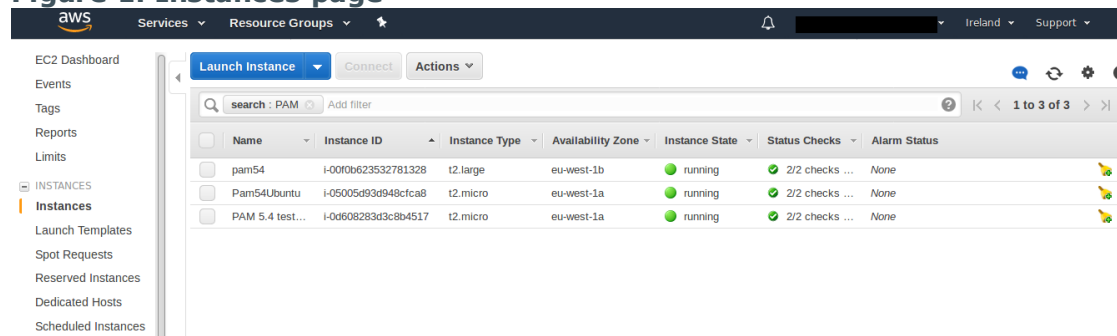
NOTE: This chapter uses a number of screenshots for illustration purposes. Note that these are added here for reference only as the look and feel (but not the contents) of the Amazon user interface may change without this guide showing the latest changes.

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)

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI) [Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

Search Privileged Session Management

My AMIs

AWS Marketplace

Community AMIs

Ownership

☒ Owned by me

☐ Shared with me

Architecture

☐ 32-bit

☐ 64-bit

Root device type

☐ EBS

☐ Instance store

Privileged Session Management 5.5 - ami-97480eee

Privileged Session Management 5.5

Root device type: ebs Virtualization type: hvm Owner: 128059300227 ENA Enabled: No

Select

64-bit

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

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Filter by: General purpose Current generation Show/Hide Columns

Currently selected: t2.large (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 8 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☒	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
☐	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
☐	General purpose	t2.xlarge	8	32	EBS only	-	Moderate	Yes
☒	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
☒	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
☒	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
☒	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
☒	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

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

5. Configure instance details:

- Select the required Virtual Private Cloud (VPC) from the **Network** list.
- 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.

- 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.
- Use the default values for all other fields or change them as required.
- 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.

- Click **Next: Add Storage**.

Figure 4: Step 3: Configure Instance Details

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances ⓘ 1 [Launch into Auto Scaling Group ⓘ](#)

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-49054e2c (default) [Create new VPC](#)

Subnet ⓘ subnet-2a811073 | Default in us-west-2c [Create new subnet](#)
4079 IP Addresses available

Auto-assign Public IP ⓘ Disable

IAM role ⓘ None [Create new IAM role](#)

Shutdown behavior ⓘ Stop

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy ⓘ Shared - Run a shared hardware instance
[Additional charges will apply for dedicated tenancy.](#)

▼ Network interfaces ⓘ

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfa ▼	subnet-2a8110 ▼	Auto-assign	Add IP

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

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

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⁱ	Device ⁱ	Snapshot ⁱ	Size (GiB) ⁱ	Volume Type ⁱ	IOPS ⁱ	Throughput (MB/s) ⁱ	Delete on Termination ⁱ	Encrypted ⁱ
Root	/dev/sda1	snap-ebe05bcc	64	Provisioned IOPS	3200	N/A	☐	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

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

Create a tag for your instance:

- Add a meaningful key-value pair that will help you later on to easily identify your instance.
- Click **Next: Configure Security Group**.

Figure 6: Step 5: Add Tags

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances ⁱ	Volumes ⁱ	
Name	demo	☒	☒	☒
Product	PSM	☒	☒	☒

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

7.

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

8. Configure security group:

- 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

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Security Group ID	Name	Description	Actions
sg-067e2a60	allowinternal	Allow traffic inside the vpc	Copy to new

Inbound rules for sg-067e2a60 (Selected security groups: sg-067e2a60)

Type	Protocol	Port Range	Source
All traffic	All	All	172.31.0.0/16

[Cancel](#) [Previous](#) [Review and Launch](#)

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

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Your instance configuration is not eligible for the free usage tier

To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

[Don't show me this again](#)

AMI Details [Edit AMI](#)

PSM54 - ami-a05edad9
PSM 5.4 formatted to 8 GiB
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.large	Variable	2	8	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security Group ID	Name	Description
sg-0abe276e	all from BBHQ	all from BBHQ

All selected security groups inbound rules

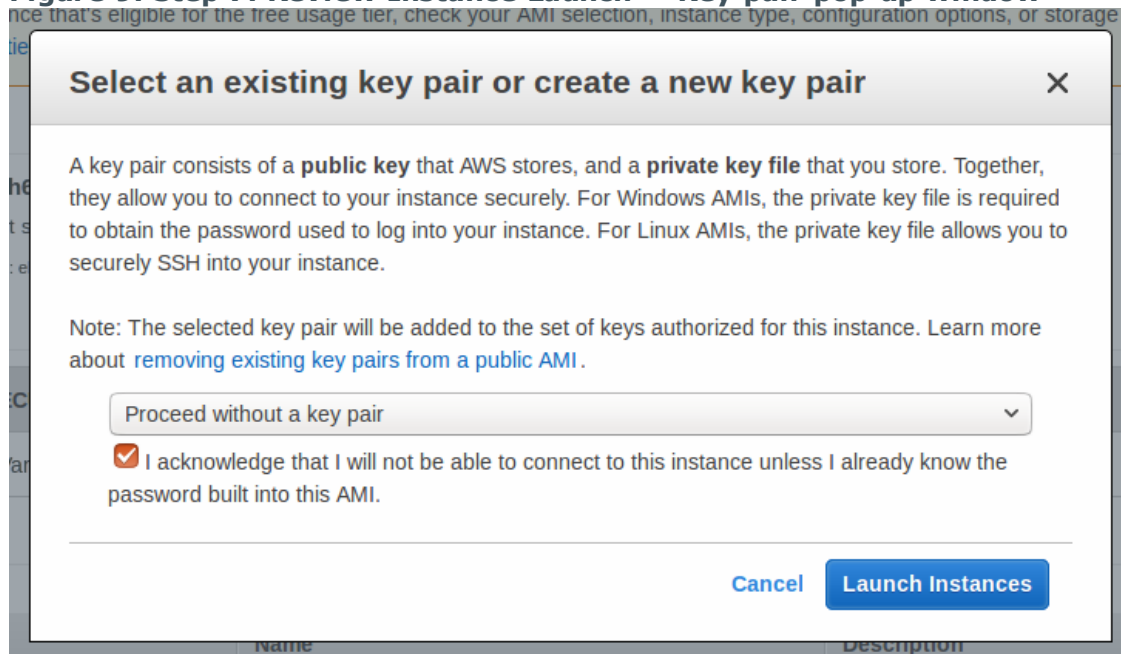
Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
All traffic	All	All	91.120.23.97/32	
All traffic	All	All	91.120.23.99/32	

[Cancel](#) [Previous](#) [Launch](#)

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

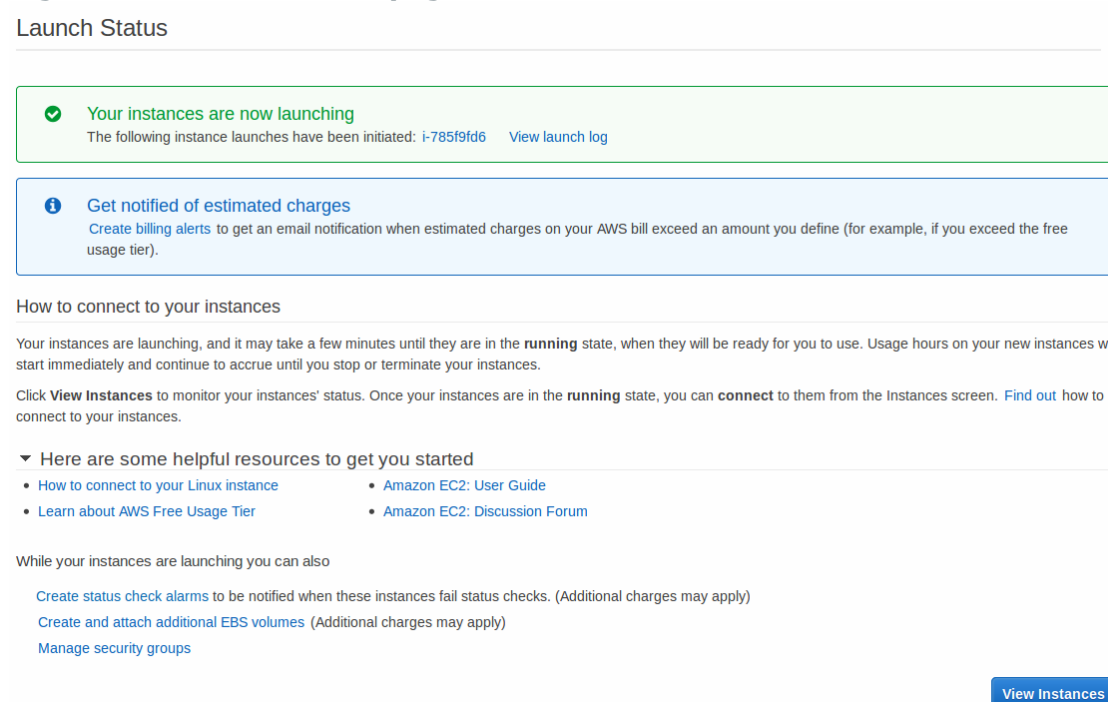
10. On the **Select an existing key pair or create a new key pair** pop-up window:
 - a. Select the **Proceed without a key pair** option.
 - b. Tick the checkbox that says "I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI".
 - c.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

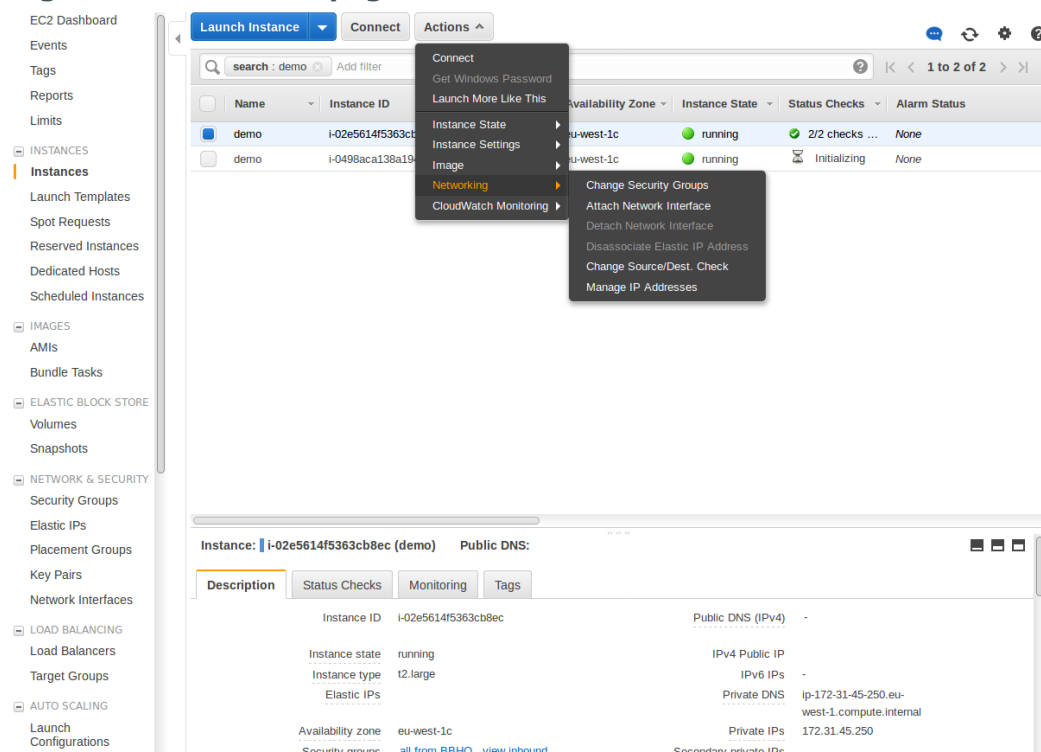
The **Instances** page comes up, which should now display the instance you have just launched. Depending on the size of the instance, installation may take up to 1-5 minutes.

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

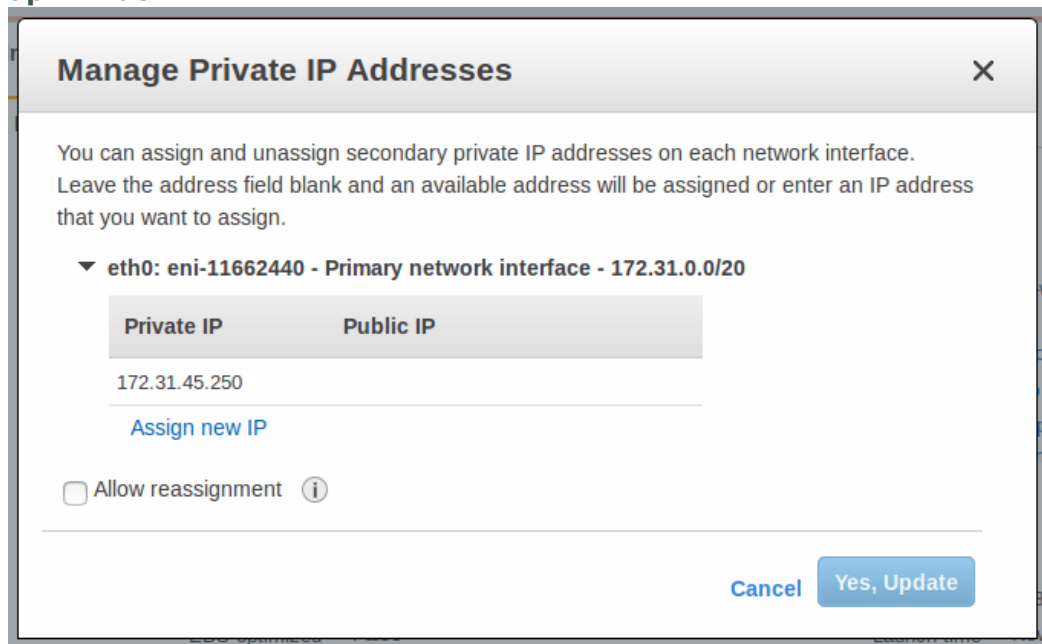


a.

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

The screenshot displays the AWS Management Console's EC2 Instances page. On the left, a navigation sidebar lists various AWS services and EC2-specific options. The main area shows a table of instances. Two instances are listed, both named 'demo'. The first instance has ID i-02e5614f5363cb8ec and is in a 'running' state. Below the table, the details for instance i-02e5614f5363cb8ec are expanded. The 'Description' tab is selected, showing instance metadata. The 'Public DNS (IPv4)' section is visible, showing the public DNS as ec2-34-242-216-31.eu-west-1.compute.amazonaws.com and the private DNS as ip-172-31-45-250.eu-west-1.compute.internal. The private IP address 172.31.45.250 is highlighted with a red box.

- 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

1. Welcome 2. License 3. Networking 4. Users 5. Certificate 6. Finish

No license file!

Networking settings

Physical interface EXT or 1:	IP address	Prefix	VLAN ID
	172.31.45.250	/ 24	
Default GW:	172.31.72.1		
Hostname:			
Domainname:			
DNS server:	172.31.0.2		
NTP server:			
Syslog server:			
SMTP server:			
Administrator's email:			
Timezone:	[select an option]		

Back Next

For detailed information on the SPS welcome wizard, see ["The Welcome Wizard and the first login"](#) in the *Administration Guide*.

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