One Identity Safeguard for Privileged Sessions 5.11

Installation Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

SPS Installation Guide
Updated - April 2019
Version - 5.11

Contents

Preface

Welcome to the One Identity Safeguard for Privileged Sessions 5 F11 Installation Guide.

This document describes how to set up the One Identity Safeguard for Privileged Sessions (SPS) hardware, and how to install SPS on certified hardware or as a virtual appliance.

Summary of contents

Introduction provides background information and describes the main purpose of the One Identity Safeguard for Privileged Sessions Installation Guide.

Package contents inventory lists the contents of the package you receive with the One Identity Safeguard for Privileged Sessions (SPS).

One Identity Safeguard for Privileged Sessions Hardware Installation Guide describes how to set up the SPS hardware.

Hardware specifications describes the hardware specifications of the SPS appliance.

One Identity Safeguard for Privileged Sessions Software Installation Guide describes how to install SPS on certified hardware.

One Identity Safeguard for Privileged Sessions VMware Installation Guide describes how to install SPS as a VMware virtual appliance.

One Identity Safeguard for Privileged Sessions Hyper-V Installation Guide describes how to install One Identity Safeguard for Privileged Sessions (SPS) as a Hyper-V virtual appliance.

Installing One Identity Safeguard for Privileged Sessions as a Kernel-based Virtual Machine describes how to install One Identity Safeguard for Privileged Sessions (SPS) as a Kernel-based Virtual Machine.

Deploying One Identity Safeguard for Privileged Sessions from the Azure Marketplace describes how to install One Identity Safeguard for Privileged Sessions (SPS) from the Microsoft Azure Marketplace.

2

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 on unpacking it and any subsequent occasions that might require the re-installation of the product.

Note that the contents of this document were previously included in the Administration Guide. This standalone guide was created to:

- Improve how information is organized in the One Identity Safeguard for Privileged Sessions documentation set.
- Make it easier for users to find information relevant to their roles, context, and how they use the product.

3

Package contents inventory

Carefully unpack all server components from the packing cartons. The following items should be packaged with the One Identity Safeguard for Privileged Sessions:

- A One Identity Safeguard for Privileged Sessions appliance, pre-installed with the latest One Identity Safeguard for Privileged Sessions firmware.
- One Identity Safeguard for Privileged Sessions accessory kit, including the following:
  - One Identity Safeguard for Privileged Sessions 5 F11 Packaging Checklist (this document).
  - GPL v2.0 license.
- Rack mount hardware (depending on appliance type).
- Power cable.

The default BIOS and IPMI passwords are in the documentation.

4

One Identity Safeguard for Privileged Sessions Hardware Installation Guide

This document describes how to set up the One Identity Safeguard for Privileged Sessions (SPS) hardware. Refer to the following documents for step-by-step instructions:

- *One Identity Safeguard for Privileged Sessions T-1*: see the *SC512 Chassis Series User's Manual, Chapter 6: Rack Installation*, available online at http://www.supermicro.com/manuals/chassis/1U/SC512.pdf.
- *One Identity Safeguard for Privileged Sessions T-4*: see the *SC815 Chassis Series User's Manual, Chapter 6: Rack Installation*, available online at http://www.supermicro.com/manuals/chassis/1U/SC815.pdf.
- *One Identity Safeguard for Privileged Sessions T-10*: see the *SC219 Chassis Series User's Manual, Chapter 5: Rack Installation*, available online at http://www.supermicro.com/manuals/chassis/2U/SC219.pdf.
- For details on how to install a single SPS unit, see Installing the SPS hardware.
- For details on how to install a two SPS units in high availability mode, see Installing two SPS units in HA mode.

Installing the SPS hardware

The following describes how to install a single SPS unit.

To install a single SPS unit

1. Unpack SPS.
2. (Optional) Install SPS into a rack with the slide rails. Slide rails are available for all SPS appliances.
3. Connect the cables.

a. Connect the Ethernet cable facing your LAN to the Ethernet connector labeled as 1. This is physical interface 1 of SPS. This interface is used for the initial configuration of SPS, and for monitoring connections. (For details on the roles of the different interfaces, see "Network interfaces" in the Administration Guide.)

b. (Optional) To use SPS across multiple physical (L1) networks, you can connect additional networks using physical interface 2 (Ethernet connector 2) and physical interface 3 (Etherner connector 3).

c. Connect an Ethernet cable that you can use to remotely support the SPS hardware to the IPMI interface of SPS. For details, see the following documents:

   For SPS T4 and T10, see the X9 SMT IPMI User's Guide. For SPS T1, see the SMT IPMI User's Guide.

   CAUTION:

   Connect the IPMI before plugging in the power cord. Failing to do so will result in IPMI failure.

   It is not necessary for the IPMI interface to be accessible from the Internet, but the administrator of SPS must be able to access it for support and troubleshooting purposes in case vendor support is needed. The following ports are used by the IPMI interface:

   - Port 623 (UDP): IPMI (cannot be changed)
   - Port 5123 (UDP): floppy (cannot be changed)
   - Port 5901 (TCP): video display (configurable)
   - Port 5900 (TCP): HID (configurable)
   - Port 5120 (TCP): CD (configurable)
   - Port 80 (TCP): HTTP (configurable)

   Access to information available only via the IPMI interface is not mandatory, but highly recommended to speed up the support and troubleshooting processes.

d. (Optional) Connect the Ethernet cable connecting SPS to another SPS node to the Ethernet connector labeled as 4. This is the high availability (HA) interface of SPS. (For details on the roles of the different interfaces, see "Network interfaces" in the Administration Guide.)

e. (Optional) The T-10 appliance is equipped with a dual-port SFP+ interface card labeled A and B. Optionally, connect a supported SFP+ module to these interfaces.

> NOTE:
>
> For a list of compatible connectors, see Linux Base Driver for 10 Gigabit Intel Ethernet Network Connection. Note that SFP transceivers encoded for non Intel hosts may be incompatible with the Intel 82599EB host chipset found in SPS.

4. Power on the hardware.
5. Change the BIOS password on the One Identity Safeguard for Privileged Sessions. The default password is `ADMIN` or `changeme`, depending on your hardware.
6. Change the IPMI password on the One Identity Safeguard for Privileged Sessions. The default password is `ADMIN` or `changeme`, depending on your hardware.

   > NOTE:
   >
   > Ensure that you have the latest version of IPMI firmware installed. You can download the relevant firmware from the One Identity Knowledge base.

   To change the IPMI password, connect to the IPMI remote console.

   > NOTE:
   >
   > If you encounter issues when connecting to the IPMI remote console, add the DNS name or the IP address of the IPMI interface to the exception list (whitelist) of the Java console. For details on how to do this, see the Java FAQ entry titled How can I configure the Exception Site List?.

7. Following boot, SPS attempts to receive an IP address automatically via DHCP. If it fails to obtain an automatic IP address, it starts listening for HTTPS connections on the `192.168.1.1` IP address.

   To configure SPS to listen for connections on a custom IP address, complete the following steps:

   a. Access SPS from the local console, and log in with username `root` and password `default`.
   b. In the Console Menu, select **Shells > Core shell**.
   c. Change the IP address of SPS:

      ifconfig eth0 <IP-address> netmask 255.255.255.0

      Replace `<IP-address>` with an IPv4 address suitable for your environment.
   d. Set the default gateway using the following command:

      route add default gw <IP-of-default-gateway>

      Replace `<IP-of-default-gateway>` with the IP address of the default gateway.
   e. Type **exit**, then select **Logout** from the Console Menu.

8. Connect to the SPS web interface from a client machine and complete the Welcome Wizard as described in "The Welcome Wizard and the first login" in the Administration Guide.

NOTE:

The Administration Guide is available on the Safeguard for Privileged Sessions Documentation page.

Installing two SPS units in HA mode

The following describes how to install SPS with high availability support.

To install SPS with high availability support

1. For the first SPS unit, complete Installing the SPS hardware.
2. For the second SPS unit, complete Steps 1-3 of Installing the SPS hardware.
3. Connect the two units with an Ethernet cable via the Ethernet connectors labeled as 4.
4. Power on the second unit.
5. Change the BIOS and IPMI passwords on the second unit. The default password is `ADMIN` or `changeme`, depending on your hardware.
6. Connect to the SPS web interface of the first unit from a client machine and enable the high availability mode. Navigate to **Basic Settings > High Availability** . Click **Convert to Cluster**, then reload the page in your browser.
7. Click **Reboot Cluster**.
8. Wait until the slave unit synchronizes its disk to the master unit. Depending on the size of the hard disks, this may take several hours. You can increase the speed of the synchronization via the SPS web interface at **Basic Settings > High Availability > DRBD sync rate limit**.

Hardware specifications

One Identity Safeguard for Privileged Sessions appliances are built on high performance, energy efficient, and reliable hardware that are easily mounted into standard rack mounts.

Table 1: Hardware specifications

Product	Redundant PSU	Processor	Memory	Capacity	RAID	IPMI
SPS T-1	No	Intel(R) Xeon(R) X3430 @ 2.40GHz	2 x 4 GB	2 x 1 TB	Software RAID	Yes
SPS T-4	Yes	Intel(R) Xeon(R) E3-1275V2 @ 3.50GHz	2 x 4 GB	4 x 2 TB	LSI MegaRAID SAS 9271-4i SGL	Yes
SPS T-10	Yes	2 x Intel(R) Xeon (R) E5-2630V2 @ 2.6GHz	8 x 4 GB	13 x 1 TB	LSI 2208 (1GB cache)	Yes

The SPS T-10 appliance is equipped with a dual-port 10Gbit interface. This interface has SFP+ connectors (not RJ-45) labeled A and B, and can be found right of the Label 1 and 2 Ethernet interfaces. If you want faster communication, for example, in case of high data load, you can connect up to two 10Gbit network cards. These cards are not shipped with the original package and have to be purchased separately.

One Identity Safeguard for Privileged Sessions Software Installation Guide

This document describes how to install the One Identity Safeguard for Privileged Sessions (SPS) software on a certified hardware. The list of certified hardware is available at One Identity.

Note that installing and reinstalling SPS can take a long time, especially for a HA cluster. There are no supported workarounds for reducing the necessary downtime. One Identity recommends testing SPS in a virtual environment, and using physical hardware only for verifying HA functionality and measuring performance.

Installing the SPS software

The following describes how to install a new SPS on a server.

Prerequisites:

When installing SPS on a physical hardware, make sure that you use a One Identity-supported appliance, and that every hard disk required for the particular appliance is inserted. Installing SPS without the required number of hard disks can cause erroneous behavior.

To install a new SPS on a server

1. Login to your support portal and download the latest One Identity Safeguard for Privileged Sessions installation ISO file. Note that you need to have partner access to download One Identity Safeguard for Privileged Sessions ISO files. If you are a partner but do not see the ISO files, you can request partner access within support portal.
2. Mount the ISO image, or burn it to a CD-ROM.
3. Connect your computer to the `IPMI` interface of SPS. For details, see the following

documents:

For SPS T4 and T10, see the X9 SMT IPMI User's Guide. For SPS T1, see the SMT IPMI User's Guide.

4. Power on the server.
5. Login to the IPMI web interface, and boot the One Identity Safeguard for Privileged Sessions installation CD on the server using a virtual CD-ROM. For details, see the following documents:

   For SPS T4 and T10, see the X9 SMT IPMI User's Guide. For SPS T1, see the SMT IPMI User's Guide.
6. When the One Identity Safeguard for Privileged Sessions installer starts, select **Installer**, press Enter, and wait until the server finishes the boot process.

   TIP:

   For testing purposes, you can speed up installation at the expense of slowing down RAID synchronization. Add the following kernel parameter to **Installer** in GRUB:

   ```
   lazy_itable_init=true
   ```

   This option defers full filesystem initialization, requiring the kernel to finish it during RAID synchronization, which slows that process down considerably. This is not recommended in a production environment.
7. Installing SPS will completely delete the contents of the hard disks. If you want to proceed installing SPS, enter`YES`to start the installation process. Depending on the size of the disks, the installation process takes from a few minutes to an hour to complete.

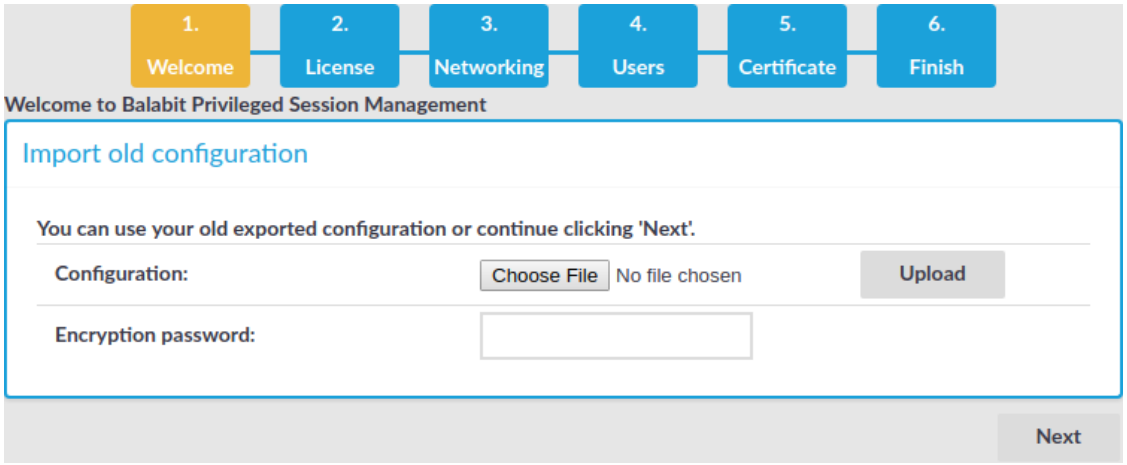
   CAUTION:

   Hazard of data loss! All data on the disks will be deleted.
8. The installer displays the following message: **Waiting for RAID sync...**, and starts to synchronize the disks of SPS.
   - You are recommended to wait until the synchronization finishes. RAID synchronization is a two-step process, the progress of the active step is indicated on the progress bar. Wait until both steps are completed. Note that this synchronization takes several hours, depending on the size of the hard disks (about 8 hours on the average).
   - To skip the RAID synchronization, press`Ctrl+Alt+Delete`to reboot SPS. Note that the system will automatically perform the synchronization after the first boot, but in this case the process will take several days.
9. When the installation is finished, the `Installation finished successfully` message is displayed. Unmount the installation media, then press `Ctrl+Alt+Delete` to reboot SPS. Wait until the system reboots and displays the IP address it accepts management connections on.
10. *If you are installing the slave node of a SPS cluster, skip this step.* Enter the IP

address displayed in the previous step into your browser and verify that the Welcome Wizard of the One Identity Safeguard for Privileged Sessions is available. (If you have to create an alias IP address for your computer that falls into the `192.168.1.0/24` subnet (for example `192.168.1.10`), see "The initial connection to SPS" in the Administration Guide.)

> **NOTE:**
>
> For details on the supported web browsers and operating systems, see "Supported web browsers and operating systems" in the Administration Guide.

Figure 1: The Welcome Wizard



11. Power off the system.

One Identity Safeguard for Privileged Sessions VMware Installation Guide

This tutorial describes the possibilities and limitations of installing One Identity Safeguard for Privileged Sessions (SPS) 5 F11 as a virtual appliance under a VMware ESXi server.

Installing SPS under VMware ESXi/ESX

The following describes how to install a new SPS under *VMware ESXi or ESX*.

To install a new SPS under VMware ESXi or ESX

1. Create the virtual machine for SPS using the following settings. Note that these settings are suitable for evaluation purposes. To test SPS under significant load, contact One Identity for recommendations.
    - Guest operating system: *Linux/Ubuntu 64-bit*
    - Allocate memory for the virtual machine. SPS requires a minimum of 4 GiB (8 GiB is recommended) of memory. The recommended size for the memory depends on the exact environment, but consider the following:
        - The base system requires 4 GiB of memory.
        - SPS requires about 1-5 MiB of memory for every active connection, depending on the type of the connection — graphical protocols require more memory.
    - The hard disk controller must be *LSI Logic Parallel*.
    - Do not use RAID for the hard disk, use the data duplication features of your virtual environment instead. That way, a single hard disk is sufficient for the system. If you need to use the built-in RAID support of SPS for some reason, use two hard disks, and SPS will automatically use them in software RAID.

> **CAUTION:**
>
> **Hazard of data loss! When you install or reinstall SPS in a virtual environment, always create new hard disks. Using existing hard disks can cause unexpected behavior and operational problems.**

- Configure a fixed size disk with at least 8 GiB space. About 5 GiB is required for the base system, the remaining disk space is used to store data. To increase the initial disk size, see Modifying the disk size of a SPS virtual appliance.

  > NOTE:
  >
  > SPS will use the network card with the lowest PCI ID as eth0 (`Physical interface 1`), the card with the second lowest PCI ID as eth1 (the `Physical interface 2`), and so on. In some cases, this might differ from the labels in the VMWare management interface, for example, it is possible that eth0 will be labeled as `Network adapter 4`, and as a result, the SPS Welcome Wizard will not be available on `Network adapter 1`.

- SPS requires at least one network card (preferably *VMXNET3*) to function. Configurations can use up to 6 network cards.

  > NOTE:
  >
  > The fourth (eth3) network card is reserved for High Availability mode by default. Therefore, make sure you enable, but do not attach, the fourth (eth3) network card to a network.

2. After creating the virtual machine, edit the settings of the machine. Set the following options:
   a. Under **Options > VMware Tools** enable the **Shutdown, Suspend, Reset** options, otherwise the SPS administrator will not be able to access these functions from the SPS web interface.
   b. Under **Options > Boot options** enable the **Force BIOS Setup** option. This is required to be able to check the system time (and modify it if needed) before installing SPS.
3. Login to your support portal and download the latest One Identity Safeguard for Privileged Sessions installation ISO file. Note that you need to have purchased SPS as a virtual appliance or have partner access to download One Identity Safeguard for Privileged Sessions ISO files. If you are a partner but do not see the ISO files, you can request partner access within support portal.
4. Mount the ISO image and boot the virtual machine. Follow the on-screen instructions to install SPS.

Limitations of SPS under VMware

The following limitations apply to running version 5 F11 of SPS under VMware:

- SPS can be installed under the following VMware versions:
  - VMware ESXi 5.5 or later.
  - VMware ESXi 6.0 or later.
  - VMware ESXi 6.5 or later.
- SPS can only use fixed disk space assigned to the virtual host, it is not possible to use on-demand disk allocation scenarios. To increase the size of the virtual disk, see Modifying the disk size of a SPS virtual appliance on page 31.
- If High Availability (HA) operation mode is required in a virtual environment, use the HA function provided by the virtual environment.
- Hardware-related alerts and status indicators of SPS may display inaccurate information, for example, display degraded RAID status.

One Identity Safeguard for Privileged Sessions Hyper-V Installation Guide

This tutorial describes the possibilities and limitations of installing One Identity Safeguard for Privileged Sessions (SPS) 5 F11 as a virtual appliance under a Hyper-V server.

Limitations of SPS under Hyper-V

Version 5 F11 of SPS has no special support for running under Hyper-V. While the basic functionality of SPS is not affected by running as a virtual appliance, the following limitations apply:

- If High Availability (HA) operation mode is required in a virtual environment, use the HA function provided by the virtual environment.
- Hardware-related alerts and status indicators of SPS may display inaccurate information, for example, display degraded RAID status.
- When running SPS under Microsoft Hyper-V, ensure that the network interfaces are actually connected to the network. When running under Hyper-V, SPS indicates on the **Basic Settings > Network > Ethernet links** page that there is a link even if the network interface is configured and enabled, but not connected to the network.
- When rebooting SPS in Hyper-V, the following critical error message may appear in the event log of the Hyper-V host:

  ```
  <Virtual machine name> was reset because an unrecoverable error occurred on a virtual processor that caused a triple fault.
  ```

  This is normal, there is no problem with SPS. For details, see Triple fault in event log shows reset of Linux virtual machines.

Installing SPS under Hyper-V

The following describes how to install a new SPS under *Hyper-V*.

To install a new SPS under Hyper-V

1. Create the virtual machine for SPS using the following settings. Note that these settings are suitable for evaluation purposes. To test SPS under significant load, contact One Identity for recommendations.
    - Choose **Generation 1** for the virtual machine.
    - Allocate memory for the virtual machine. SPS requires a minimum of 4 GiB (8 GiB is recommended) of memory. The recommended size for the memory depends on the exact environment, but consider the following:
        - The base system requires 4 GiB of memory.
        - SPS requires about 1-5 MiB of memory for every active connection, depending on the type of the connection — graphical protocols require more memory.
    - Do not use RAID for the hard disk, use the data duplication features of your virtual environment instead. That way, a single hard disk is sufficient for the system. If you need to use the built-in RAID support of SPS for some reason, use two hard disks, and SPS will automatically use them in software RAID.

      CAUTION:

      Hazard of data loss! When you install or reinstall SPS in a virtual environment, always create new hard disks. Using existing hard disks can cause unexpected behavior and operational problems.
    - Configure a fixed size disk with at least 8 GiB space. About 5 GiB is required for the base system, the remaining disk space is used to store data. To increase the initial disk size, see Modifying the disk size of a SPS virtual appliance.

      NOTE:

      SPS will use the network card with the lowest PCI ID as eth0 (`Physical interface 1`), the card with the second lowest PCI ID as eth1 (the `Physical interface 2`), and so on. In some cases, this might differ from the labels in the Hyper-V management interface, for example, it is possible that eth0 will be labeled as `Network adapter 4`, and as a result, the SPS Welcome Wizard will not be available on `Network adapter 1`.
    - SPS requires at least one network card to function. Configurations can use up to 6 network cards.

NOTE:

The fourth (eth3) network card is reserved for High Availability mode by default. Therefore, make sure you enable, but do not attach, the fourth (eth3) network card to a network.

CAUTION:

Hyper-V offers two kinds of virtual Network Adapters (NICs): Legacy and Synthetic. Due to a known issue (Hyper-V network adapters are mapped to a different eth on every boot), using Legacy and Synthetic NICs within the same configuration will result in improper network setup. If you have to use more than one NICs, we recommend using only Legacy NICs.

2. Login to your support portal and download the latest One Identity Safeguard for Privileged Sessions installation ISO file. Note that you need to have purchased SPS as a virtual appliance or have partner access to download One Identity Safeguard for Privileged Sessions ISO files. If you are a partner but do not see the ISO files, you can request partner access within support portal.
3. Mount the ISO image and boot the virtual machine. Follow the on-screen instructions to install SPS.

Installing One Identity Safeguard for Privileged Sessions as a Kernel-based Virtual Machine

This tutorial describes the possibilities and limitations of installing One Identity Safeguard for Privileged Sessions (SPS) 5 F11 as a virtual appliance using the Kernel-based Virtual Machine (KVM) solution.

Installing SPS as a Kernel-based Virtual Machine

The following describes how to install a new SPS as a Kernel-based Virtual Machine.

To install a new SPS as a Kernel-based Virtual Machine

1. Create the virtual machine for SPS using the following settings. Note that these settings are suitable for evaluation purposes. To test SPS under significant load, contact One Identity for recommendations.
    - Guest operating system: *Linux/Ubuntu 64-bit*
    - Allocate memory for the virtual machine. SPS requires a minimum of 4 GiB (8 GiB is recommended) of memory. The recommended size for the memory depends on the exact environment, but consider the following:
        - The base system requires 4 GiB of memory.
        - SPS requires about 1-5 MiB of memory for every active connection, depending on the type of the connection — graphical protocols require more memory.
    - The hard disk controller must be *virtio*.
    - Do not use RAID for the hard disk, use the data duplication features of your virtual environment instead. That way, a single hard disk is sufficient for the

system. If you need to use the built-in RAID support of SPS for some reason, use two hard disks, and SPS will automatically use them in software RAID.

> **CAUTION:**
>
> **Hazard of data loss! When you install or reinstall SPS in a virtual environment, always create new hard disks. Using existing hard disks can cause unexpected behavior and operational problems.**

- Configure a fixed size disk with at least 8 GiB space. About 5 GiB is required for the base system, the remaining disk space is used to store data. To increase the initial disk size, see Modifying the disk size of a SPS virtual appliance.
- SPS requires 4 network cards, all of them must be *virtio*.

  > NOTE:
  >
  > SPS will use the network card with the lowest PCI ID as eth0 (`Physical interface 1`), the card with the second lowest PCI ID as eth1 (the `Physical interface 2`), and so on. In some cases, this might differ from the labels in the VMWare management interface, for example, it is possible that eth0 will be labeled as `Network adapter 4`, and as a result, the SPS Welcome Wizard will not be available on `Network adapter 1`.

  Configure unused network cards — at least the fourth (eth3) — to use internal NAT.
- To index connections without significant delay, add two CPU cores to the virtual machine. Note that these settings are suitable for evaluation purposes. To test SPS under significant load, contact One Identity for recommendations. The resource requirements of indexing depend heavily on the amount and type of the indexed traffic, and can also require using external indexer hosts (for details on external indexers, see "Configuring external indexers" in the Administration Guide).

2. Login to your support portal and download the latest One Identity Safeguard for Privileged Sessions installation ISO file. Note that you need to have purchased SPS as a virtual appliance or have partner access to download One Identity Safeguard for Privileged Sessions ISO files. If you are a partner but do not see the ISO files, you can request partner access within support portal.
3. Mount the ISO image and boot the virtual machine. Follow the on-screen instructions to install SPS.

Limitations of SPS under KVM

The following limitations apply to running version 5 F11 of SPS under KVM:

- SPS can be installed under KVM on most modern Linux distributions. One Identity currently tests the following KVM version:

  ```
  # virsh version
  Compiled against library: libvirt 1.2.17
  Using library: libvirt 1.2.17
  Using API: QEMU 1.2.17
  Running hypervisor: QEMU 1.5.3
  ```

- SPS can only use fixed disk space assigned to the virtual host, it is not possible to use on-demand disk allocation scenarios.
- If High Availability (HA) operation mode is required in a virtual environment, use the HA function provided by the virtual environment.
- Hardware-related alerts and status indicators of SPS may display inaccurate information, for example, display degraded RAID status.

Deploying One Identity Safeguard for Privileged Sessions from the Azure Marketplace

This guide provides detailed descriptions for deploying One Identity Safeguard for Privileged Sessions (SPS) from the Microsoft Azure Marketplace.

Before you start:

Before you start evaluating SPS, make sure you understand what SPS is and how it works. This information can greatly help you get SPS operational. Read the following:

- "Introduction" in the Administration Guide
- "The concepts of SPS" in the Administration Guide

Prerequisites

The following prerequisites must be met to deploy SPS in Microsoft Azure:

- You have a valid One Identity Safeguard for Privileged Sessions license. When deployed from the Microsoft Azure Marketplace, the 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 Sales Team.
- Microsoft recommends to use the Azure Resource Manager (ARM) deployment model. When you install SPS from the Azure Marketplace, SPS supports only this deployment method. If you need to deploy SPS into and infrastructure that uses the Classic deployment model, contact your One Identity sales representative.
- You have a Microsoft Azure account.

Limitations

The following limitations apply to SPS when you deploy it from the Microsoft Azure Marketplace.

CAUTION:

Do not export or import configuration between a physical SPS deployment and a virtual one. Because of the differences and limitations between physical and virtual appliances, configure the virtual appliance from scratch to ensure proper functionality. When you migrate a virtual SPS to another one, you can export and import the configuration.

- Root login is not available on the console.
- SSH access is only available after you have completed the Welcome Wizard.
- Currently, the data that is entered during the provisioning phase (for example username, IP address) of creating the virtual machine in Azure is not transferred to SPS. Therefore, only the data entered in the Welcome Wizard will be used.
- By default, you can only use Physical interface 1 (eth0) of SPS, with a single IP address. Aside from changing the IP address of SPS, do not modify other interface-related settings (additional logical interfaces, IP forwarding, and so on) on the **Basic Settings > Network** page of SPS.

  The number of interfaces you can use depends on the size of your Azure VM. If your VM allows you to use multiple interfaces, you can configure multiple interfaces in SPS. For details, see VM with multiple NICs.
- The **Seal the box** functionality is not available.
- The High Availability support of SPS was designed to work between two physical SPS appliances. This feature is not available in Azure environments. For further details, see the High Availability and redundancy in Microsoft Azure.
- Due to Azure requirements, an additional 5-minute delay has been added to the boot process. This ensures that the root device appears in the system.
- The size of the hard disk in Azure is 100 Gb. You cannot extend this virtual disk size later, nor can you write to Samba or other disks. In case you run out of disk space, either configure a **Backup policy** and an **Archive policy** if you have a server for this purpose, or configure a **Cleanup policy** that deletes the audit trails at certain time intervals. For details, see "Data and configuration backups" in the Administration Guide and "Archiving and cleanup" in the Administration Guide.
- SPS currently cannot receive its IP address using DHCP. Make sure that:
  - The IP address you have configured in Azure and the IP address that you configure for SPS for the **Physical interface 1** on the Networking settings part of the Welcome Wizard are the same. Otherwise, you will not be able to access SPS.
  - You set the internal IP static on the Network Interfaces tab of the Virtual

Machine.

- Do not assign a public IP address to SPS, use SPS as a component of your internal infrastructure. If you absolutely must configure Welcome Wizard from a publicly accessible IP address, note that SPS will be publicly accessible. If you assign a public IP to the web management interface, consider the following:
  - Select a complex passphrase.
  - Limit access to the management interface based on the source IP address, and make sure that brute-force protection for the administrator web login is enabled (they are enabled by default). For details, see "Configuring user and administrator login addresses" in the Administration Guide.
  - Configure an email alert or SNMP trap for administrator logon events. For details, see "Configuring e-mail alerts" in the Administration Guide and "Configuring SNMP alerts" in the Administration Guide.
  - Forward the logs of SPS to a log server (for example, to a syslog-ng server, or an syslog-ng Store Box appliance) so that if the local logs are compromised, you still have an authentic copy of the original logs.
  - For security reasons, disable SSH access to SPS when it is not needed. Accessing the SPS host directly using SSH is not recommended or supported, except for troubleshooting purposes. If you enable SSH access, restrict the clients that can access SPS based on their source IP address, and make sure that brute-force protection is enabled (they are enabled by default). For details, see "Enabling SSH access to the SPS host" in the Administration Guide.
  - To prevent unauthorized access to the audit trail files recorded on SPS, configure proper access control rules for the user groups and encrypt every audit trail. If you use encryption, store your keys in the personal or in the temporary key store. For details, see "Encrypting audit trails" in the Administration Guide,
- Upgrading SPS in Azure is the same as upgrading a physical appliance: you have to upload the firmware on the SPS web interface. For detailed instructions, see Upgrade Guide.

Deploy One Identity Safeguard for Privileged Sessions from the Microsoft Azure Marketplace

Purpose:

The following describes how to have a One Identity Safeguard for Privileged Sessions running in Microsoft Azure.

To have a One Identity Safeguard for Privileged Sessions running in Microsoft Azure

1. **Deploy One Identity Safeguard for Privileged Sessions from the Microsoft Azure Marketplace**

   Create and configure a One Identity Safeguard for Privileged Sessions virtual machine (VM) in the Azure portal. For details, see the Microsoft Azure documentation, here we just describe the SPS-specific settings.

   a. Login to the Azure portal, select **One Identity Safeguard for Privileged Sessions** from the Azure Marketplace, then click **Create**.

   b. Fill the required fields of the **Basics** blade. Note that you must fill the **User name** and **Authentication Password/SSH public key** fields, but SPS will not actually use these settings (SPS will use the parameters you configure in the SPS Welcome Wizard).

   c. Choose a size for the VM. If you want to use this machine in production and need help about sizing or architecture design, contact your One Identity sales representative.

      The number of interfaces you can use depends on the size of your Azure VM. If your VM allows you to use multiple interfaces, you can configure multiple interfaces in SPS. For details, see VM with multiple NICs.

   d. On the **Settings** blade, disable monitoring.

   e. When the deployment is finished, navigate to the network settings of the new VM in the Azure portal. Change the IP address of the SPS network interface to Static, and note down the IP address and the hostname (you will need it in the SPS Welcome Wizard).

   f. If you want to backup or archive data from SPS into Azure, create an Azure File Share. Note down the following information of the file share, because you will need it to configure SPS backups and archiving: `URL`, `Username`, `Password`.

      CAUTION:

      If you have multiple SPS VMs, make sure to use a separate file share for each SPS.

2. **Complete the SPS Welcome Wizard**

   Complete the SPS Welcome Wizard (for details, see "Configuring SPS with the Welcome Wizard" in the Administration Guide). Note the following points specific for Azure deployments. When configuring the network settings of SPS note the following points.

CAUTION:

Do not export or import configuration between a physical SPS deployment and a virtual one. Because of the differences and limitations between physical and virtual appliances, configure the virtual appliance from scratch to ensure proper functionality. When you migrate a virtual SPS to another one, you can export and import the configuration.

a. Into the **Physical interface EXT or 1 — IP address** field, enter the static IP address of the SPS VM that you set on the Azure portal.

b. **Default GW**: The default gateway is usually the first address in a subnet (for example, if your subnet is `10.7.0.0/24`, then the gateway will be `10.7.0.1`).

c. **Hostname**: Use the hostname you have configured for the SPS VM on the Azure portal.

d. **DNS server**: You can use any DNS server that the SPS VM can access, even public ones.

3. **Configure SPS**

Login to SPS and configure it.

a. Configure backups for SPS. For backup and archiving purposes One Identity recommends the built-in file shares of Azure. For details on configuring backups, see "Data and configuration backups" in the Administration Guide.

b. Configure archiving for SPS. For backup and archiving purposes One Identity recommends the built-in file shares of Azure. For details on configuring backups, see "Archiving and cleanup" in the Administration Guide. Configuring Archiving policy is highly recommended: because if the disk of the VM fills up, SPS stops working.

c. Configure a server: set up a host that is on the same subnet as SPS, and enable Remote Desktop (RDP) or Secure Shell (SSH) access to it.

d. Configure a connection on SPS to forward the incoming RDP or Secure Shell (SSH) connection to the host and establish a connection to the host. See "Logging in to SPS and configuring the first connection" in the Administration Guide for details.

e. Replay your session in the browser. See "Replaying audit trails in your browser in Search (classic)" in the Administration Guide for details.

In case you have questions about SPS, or need assistance, contact your One Identity representative.

High Availability and redundancy in Microsoft Azure

In a Microsoft Azure deployment, the high-availability and redundancy of the SPS appliance is provided by the Microsoft Azure infrastructure, according to the Azure Storage SLA.

Redundancy

The data in your Microsoft Azure storage account is always replicated to ensure durability and high availability, meeting the Azure Storage SLA. The exact type of replication depends on your storage account settings, but every disk is stored in 3 copies.

For details, see Locally redundant storage in the *Azure Storage replication* document, and Service Healing - Auto-recovery of Virtual Machines.

High Availability

If a hardware failure occurs, Azure moves the Virtual Machine to another location and restarts it in 5-15 minutes. In case you require higher SLA, you are recommended to deploy two standalone SPS nodes into an availability set. Note that to deploy two active SPS nodes as an availability set, you must purchase two standalone SPS licenses.

For details, see Locally redundant storage in the *Azure Storage replication* document, and Service Healing - Auto-recovery of Virtual Machines.

Virtual appliance maintenance

Modifying the disk size of a SPS virtual appliance

SPS can only use fixed disk space assigned to the virtual host. If you must increase the size of the virtual disk, complete the following steps. Online disk resize can grow the filesystem up to 1024x size of the original size.

Prerequisites:

You can resize the disk that way only if you originally installed SPS version 5 LTS or later. This method will not work if you upgraded to 5 LTS from an earlier version.

To modify the disk size of a SPS virtual appliance

1. **Warning! Hazard of data loss!**

   Create a full system backup (configuration and data backup). For detailed instructions, see "Data and configuration backups" in the Administration Guide.
2. Power down the virtual machine.
3. Increase the storage size.
4. Power on the SPS virtual machine.
5. Login to SPS as root locally (or remotely using SSH) to access the Console menu.
6. Select **Shells > Boot Shell**.
7. Issue the following command: **parted /dev/Xda resizepart**

   Letter X might vary on different systems. Usually it is 's' or 'v'. Check your system before issuing this command.
8. Answer the on-screen questions with the following answers:

- **Fix/Ignore?** > `fix`
- **Partition number?** > `4`
- **Warning: Partition /dev/sda4 is being used. Are you sure you want to continue? Yes/No?** > `yes`
- **End?** > `-0`
- **Fix/Ignore?** > `fix`

For example:

```
(boot/master/ip99)root@scb1:~# parted /dev/sda resizepart
Warning: Not all of the space available to /dev/sda appears to be used, you can
fix the GPT to use all of the space (an extra 4194304 blocks) or continue with
the current setting?
Fix/Ignore? fix
Partition number? 4
Warning: Partition /dev/sda4 is being used. Are you sure you want to continue?
Yes/No? yes
End?  [22.5GB]? -0
Information: You may need to update /etc/fstab.
```

9. Issue the following command: **resize2fs /dev/Xda4**

   Letter `X` might vary on different systems. Usually it is 's' or 'v'. Check your system before issuing this command.

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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

Third-party contributions

This appendix includes the open source licenses and attributions applicable to One Identity Safeguard for Privileged Sessions.