One Identity Safeguard for Privileged Sessions 5 LTS

Packaging Checklist

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 Packaging Checklist
Updated - November 2018
Version - 5 LTS

Contents

A. Package contents inventory **4**

B. One Identity Safeguard for Privileged Sessions Hardware Installation Guide **5**

C. Hardware specifications **9**

About us **10**

Contacting us 10

Technical support resources 10

A. Package contents inventory

[1]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 LTS 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.

B. 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 Procedure B.1, "Installing the SPS hardware".
- For details on how to install a two SPS units in high availability mode, see Procedure B.2, "Installing two SPS units in HA mode".

Procedure B.1. Installing the SPS hardware

Purpose:

To install a single SPS unit, complete the following steps.

Steps:

1. Unpack SPS.
2. *Optional step*: 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 One Identity Safeguard for Privileged Sessions - Technical Documentation.)

b. *Optional step:* 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 IMPI 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 step:* 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 One Identity Safeguard for Privileged Sessions - Technical Documentation.)

e. *Optional step:* 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 Balabit 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 One Identity Safeguard for Privileged Sessions - Technical Documentation.

   NOTE:

   The One Identity Safeguard for Privileged Sessions - Technical Documentation is available on the One Identity Documentation page.

Procedure B.2. Installing two SPS units in HA mode

Purpose:

To install SPS with high availability support, complete the following steps.

Steps:

1. For the first SPS unit, complete Procedure B.1, "Installing the SPS hardware".
2. For the second SPS unit, complete Steps 1-3 of Procedure B.1, "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**.

C. Hardware specifications

SPS appliances are built on high performance, energy efficient, and reliable hardware that are easily mounted into standard rack mounts.

Table C.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

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