One Identity Safeguard for Privileged Sessions 7.0.1.1 LTS

Packaging Checklist

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.

SPSPackaging Checklist
Updated - 05 January 2023, 13:06

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

Contents

Package contents inventory **4**

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

Installing the SPS hardware 5

Installing two SPS units in HA mode 8

Hardware specifications **9**

About us **10**

Contacting us **11**

Technical support resources **12**

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 7.0.1.1 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.

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:

- *Safeguard Sessions Appliance 3000*: see the *SC113 Chassis Series User's Manual, Chapter 6: Rack Installation*, available online at https://www.supermicro.com/manuals/chassis/1U/SC113.pdf.
- *Safeguard Sessions Appliance 3500*: see the *SuperServer 1029U-T Series User's Manual, Chapter 2: Server Installation*, available online at https://www.supermicro.com/manuals/superserver/1U/MNL-1973.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 (Ethernet 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 Safeguard Sessions Appliance 3000 and 3500, see the X9 SMT IPMI User's Guide.

   CAUTION:

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

   CAUTION: SECURITY HAZARD!

   The IPMI, like all out-of-band management interfaces, has known vulnerabilities that One Identity cannot fix or have an effect on. To avoid security hazards, One Identity recommends that you only connect the IPMI to well-protected, separated management networks with restricted accessibility. Failing to do so may result in an unauthorized access to all data stored on the SPS appliance. Data on the appliance can be unencrypted or encrypted, and can include sensitive information, for example, passwords, decryption keys, private keys, and so on.

   For more information, see Best Practices for managing servers with IPMI features enabled in Datacenters.

   NOTE: The administrator of SPS must be authorized and able to access the IPMI for support and troubleshooting purposes in case vendor support is needed.

   The following ports are used by the IPMI:

   - Port 22 (TCP): SSH (configurable)
   - Port 80 (TCP): Web (configurable)
   - Port 161 (UDP, TCP): SNMP (configurable)
   - Port 443 (TCP): Web SSL (configurable)
   - Port 623 (UDP): Virtual Media (configurable)
   - Port 5900 (TCP): IKVM Server (configurable)
   - Port 5985 (TCP): Wsman (configurable)

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 Safeguard Sessions Appliance 3500 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 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. Select **Shells > Core shell** in the Console Menu.
   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

CAUTION:

Creating a High-availability (HA) node pair from different types of hardware is not possible. The primary and the secondary HA nodes have to run on the same type of hardware.

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

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

For detailed hardware specifications of your appliance, see "Hardware specifications" in the Installation 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