



One Identity Safeguard for Privileged Passwords 7.0.5.1 LTS

Appliance Setup Guide

Copyright 2024 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.**

Safeguard for Privileged Passwords Appliance Setup Guide
Updated - 14 August 2024, 15:11

For the most recent documents and product information, see [Online product documentation](#).

Contents

Hardware appliance	4
Package contents	4
Front and back panels	5
Operating conditions and regulatory compliance	6
Setting up the hardware appliance	8
Warnings and precautions	11
Standardized warning statements for AC systems	12
Virtual machine	15
Using the virtual appliance and web management console	15
Setting up the virtual appliance	17
Support Kiosk	21
Virtual appliance backup and recovery	23
Completing the appliance setup	25
Cloud deployments	28
Cloud deployment considerations	28
AWS deployment	30
Azure deployment	32
Virtual appliance backup and recovery	34
System requirements and versions	36
Web client system requirements	37
Web management console system requirements	37
Supported platforms	38
Licenses	44
Long Term Support (LTS) and Feature Releases	46
About us	48
Contacting us	49
Technical support resources	50

Hardware appliance

Safeguard for Privileged Passwords can be run from:

- The One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance or 2000 Appliance (hardware)
- A virtual machine
- The cloud

This section covers the background and steps you need to set up the hardware appliance for the first time.

[Package contents](#)

[Front and back panels](#)

[Operating conditions and regulatory compliance](#)

[Setting up the hardware appliance](#)

[Warnings and precautions](#)

[Standardized warning statements for AC systems](#)

Package contents

In addition to this guide, the One Identity Safeguard for Privileged Passwords package contents includes the following:

1. One Identity Safeguard for Privileged Passwords appliance
2. (2) Country Specific Power cables*
3. Rails
4. Short Rail Bracket Sets
5. Rail Screws
6. 5 foot Ethernet cable
7. 6 foot Serial Cable

8. USB to 2.0 Serial Cable

9. Port Blockers

*The included power cords are approved by use only in specific countries or regions. Before using a power cord, verify that it is rated and approved for use in your location. The power cord is for AC mains installation only.

If any items are missing from your package, contact Support at: <https://support.oneidentity.com>

Front and back panels

The following diagrams show the front and back panels on the One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance.

Figure 1: Front and back panel of 4000 Appliance

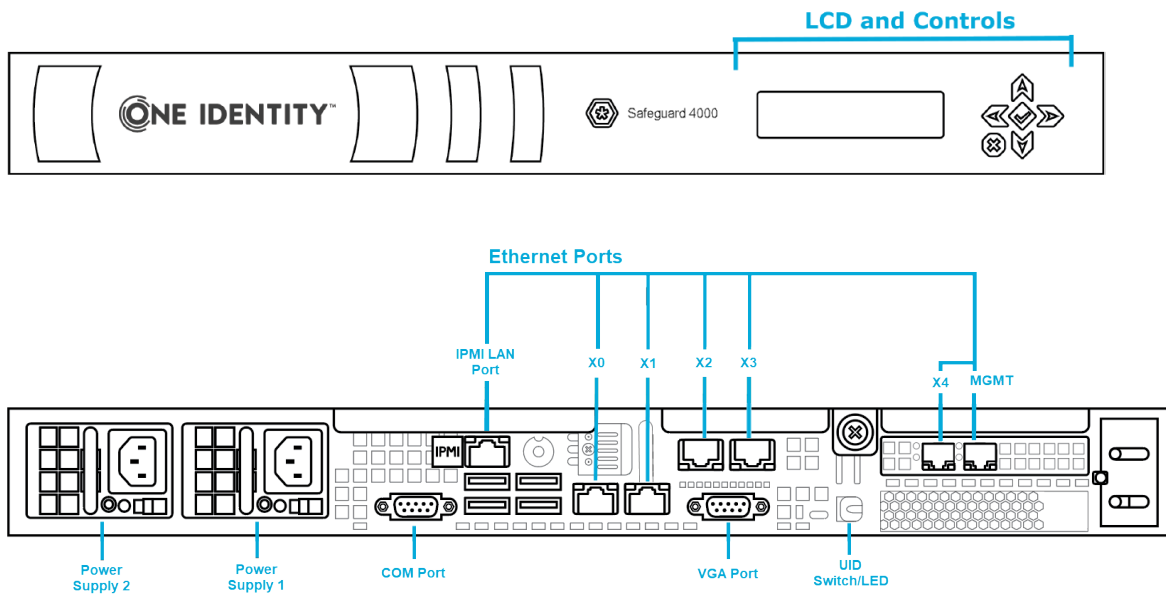
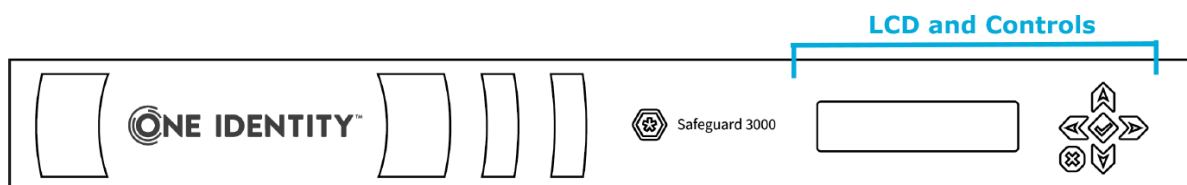


Figure 2: Front and back panel of 3000 Appliance



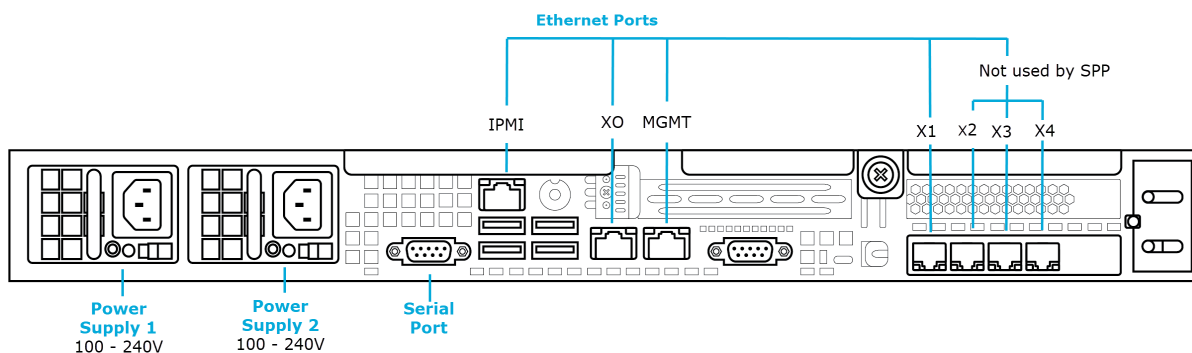
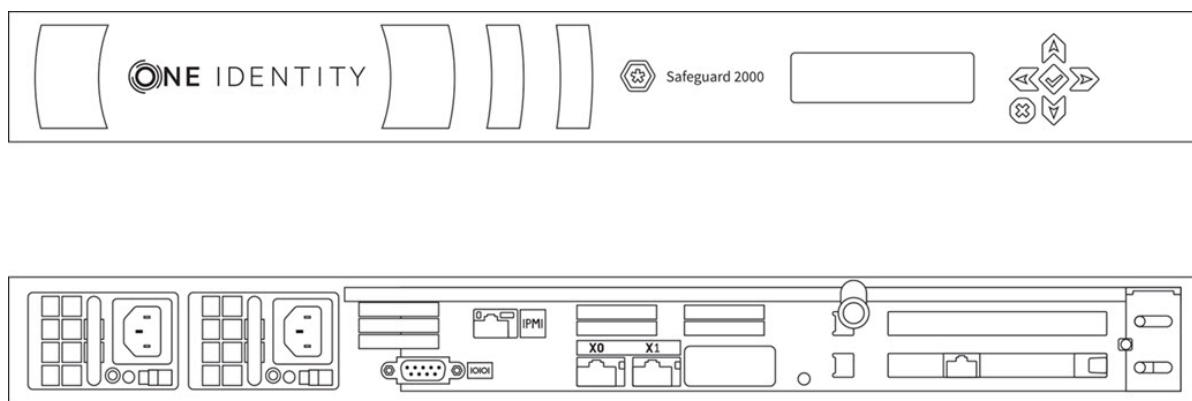


Figure 3: Front and back panel of 2000 Appliance



Operating conditions and regulatory compliance

Operating conditions (運行條件)

Input (輸入/輸入): 100-140 / 180-240 Vac, 50-60 Hz, 8.5-6.0 / 5.0-3.8 A

Operating Temperature (工作溫度): 5 C to 35 C

Altitude of Operation (m)...: Up to 2000 m (操作高度(m): 最高2000 m)

Regulatory compliance

Electromagnetic Emissions: FCC Class A, EN 55032 Class A, EN 61000-3-2/-3-3, CISPR 32 Class A, VCCI Class A

Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)

Safety: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)

FCC warning

This equipment has been tested and found to comply with the regulations for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

CE Mark warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Taiwan BSMI Class A Warning Statement

This is a Class A Information Product, when used in residential environment, it may cause radio frequency interference, under such circumstances, the user may be requested to take appropriate countermeasures.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Setting up the hardware appliance

⚠ CAUTION: To maximize security, restrict the access to MGMT interface to as few users as possible. The Management web kiosk gives access to functions without authentication, such as pulling a support bundle or rebooting the appliance.

Follow these steps to set up and configure the One Identity Safeguard for Privileged Passwords Appliance.

Step 1: Before you start

For the 3000 and 2000 appliances, ensure that you install the .NET Framework 4.6 (or later) on your management host. 4000 appliances do not have this requirement since they ship with the 7.0 version of One Identity Safeguard for Privileged Passwords.

Check the [One Identity Support site](#) and install the latest version of the software.

Step 2: Prepare for installation

Gather the following items before you start the appliance installation process:

- Laptop
- IP address
- IP subnet mask
- IP gateway
- DNS server address
- NTP server address
- One Identity Safeguard for Privileged Passwords license

If you purchased One Identity Safeguard for Privileged Passwords, the appropriate license files should have been sent to you via email. If you have not received an email or need it to be resent, visit <https://support.oneidentity.com/contact-us/licensing>. If you need to request a trial key, please send a request to sales@oneidentity.com or call +1-800-306-9329.

Step 3: Rack the appliance

Prior to installing the racks for housing the appliance, see [Warnings and precautions](#).

Step 4: Power on the appliance

Prior to powering up the appliance, see [Standardized warning statements for AC systems](#).

The One Identity Safeguard for Privileged Passwords Appliance includes dual power supplies for redundant AC power and added reliability.

1. Plug the power cords to the power supply sockets on the appliance back and then connect the cords to AC outlets.

TIP: As a best practice, connect the two power cords to outlets on different circuits. One Identity recommends using an UPS on all appliances.

2. Press the **Green check mark** button on the front panel of the appliance for NO MORE THAN one second to power on the appliance.

CAUTION: Once the Safeguard for Privileged Passwords Appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.

You can use the **Red X** button to shut down the appliance. Once the Safeguard for Privileged Passwords Appliance is booted, press and hold the **Red X** button for four seconds until it displays POWER OFF.

NOTE: If the Safeguard for Privileged Passwords Appliance is not yet booted, it may be necessary to press the **Red X** button for up to 13 seconds.

CAUTION: Once the Safeguard for Privileged Passwords Appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.

Step 5: Connect the management host to the appliance

The port used for a secure first-time configuration of the appliance is **MGMT**. This IP address is a fixed address that cannot be changed. It will always be available in case the primary interface becomes unavailable. The **MGMT** IP address is: 192.168.1.105.

The primary interface that connects your appliance to the network is **X0**. You must change the primary interface IP to match your network configuration. The default **X0** IP is: 192.168.0.105.

The appliance can take up to five minutes to boot up. In addition, ping replies have been disabled on the appliance, so you will not be able to ping this secure appliance.

1. Connect an Ethernet cable from the laptop to the **MGMT** port on the back of the appliance.
2. Set the IP address of the laptop to 192.168.1.100, the subnet mask to 255.255.255.0, and no default gateway.


Step 6: Log in to Safeguard for Privileged Passwords

1. Open a browser on the laptop and connect to the IP address of the **MGMT** port <https://192.168.1.105>.

If you have problems accessing the configuration interface, check your browser Security Settings or try using an alternate browser.

2. Accept the certificate and continue. This is only safe when using an Ethernet cable connected directly to the appliance.
3. Log in to the Safeguard for Privileged Passwords web client using the Bootstrap Administrator account:
 - User name: **admin**
 - Password: **Admin123**

The Bootstrap Administrator is a built-in account that allows you to get the appliance set up for first-time use. To keep your Safeguard for Privileged Passwords Appliance secure, change the default password for the Bootstrap Administrator's account. For more information, see [Completing the appliance setup](#).

4. Configure the primary network interface (X0):
 - On the **Appliance Configuration** page, configure the following. Click the  **Edit** icon to modify these settings.
 - **Time:** Enable NTP and set the primary NTP server; if desired, set the secondary NTP server, as well. Click **Save**. By default, the NTP server is set to pool.ntp.org.
 - **Network (X0):**
 - Enter the appliance's IPv4 and/or IPv6 address information (IP address, Subnet Mask, Gateway). Directory or network scans are supported for IPv4 but not IPv6.
 - Enter the DNS server address.
 - Optional, enter the DNS suffixes.
 - Click **Save**.

NOTE: Starting with Safeguard for Privileged Passwords 6.9, the Network Interface (X1) can be used to add additional virtual network adapters associated with the X1 ethernet port to enable VLAN support.

5. Log in to the web client to complete the next steps. For more information, see [Completing the appliance setup](#).

Step 7: Connect the appliance to the network

Connect an Ethernet cable from your primary interface (X0) on the appliance to your network.

Step 8. After clustering, change the trusted servers, CORS, and redirects setting

As a best practice, after you have created your Safeguard for Privileged Passwords cluster (or if just using a single VM), change the Trusted Servers, CORS and Redirects setting to the empty string or a list of values to integration applications you wish to allow. For more details, see the *Safeguard for Privileged Passwords Administration Guide*, Trusted Servers, CORS and Redirects.

Warnings and precautions

The following precautions must be taken for proper installation.

Rack precautions

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In a single-rack assembly, stabilizers should be attached to the rack. In a multi-rack assembly, the racks should be coupled together.
- Always ensure the rack is stable before extending a component from the rack.
- Extend only one component at a time; extending two or more components simultaneously may cause the rack to become unstable.

Component precautions

- Review the electrical and general safety precautions. For more information, see [Standardized warning statements for AC systems](#) on page 12.
- Determine the placement of each component in the rack BEFORE you install the rails.
- Install the heaviest components on the bottom of the rack first, and then work up.
- Use a regulating uninterruptible power supply (UPS) to protect the component from power surges, voltage spikes, and to keep your system operating in case of a power failure.
- Allow the hot plug SATA drives and power supply modules to cool before touching them.
- Always keep the rack's front door and all panels and components on the appliance closed when not servicing to maintain proper cooling.

Appliance and mounting considerations

The following conditions are required for proper installation.

Ambient operating temperature

If installed in a closed or multi-rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (T_{mra}).

Reduced airflow

Mount the equipment into the rack so that the amount of airflow required for safe operation is not compromised.

Mechanical loading

Mount the appliances evenly in the rack in order to prevent a hazardous condition due to uneven mechanical loading.

Circuit overloading

Consideration must be given to the connection of the equipment to the power supply circuit. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern. Do not overload the circuit.

Reliable ground

Reliable grounding of rack-mounted equipment must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention must be given to power supply connections other than the direct connections to the branch circuit, such as power strips.

Standardized warning statements for AC systems

The following statements are industry-standard warnings, provided to warn the user of situations that have the potential for bodily injury. Should you have questions or experience difficulty, contact One Identity technical support for assistance. Only certified technicians should attempt to install or configure components.

Read this appendix in its entirety BEFORE installing or configuring components in the One Identity Safeguard for Privileged Passwords Appliance.

NOTE: These warning statements are also available in multiple languages on the One Identity support site:

<https://support.oneidentity.com/one-identity-safeguard/2.0/technical-documents>.

Warning definition

⊗ WARNING: This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Installation instructions

- ⊗ **WARNING:** Read the installation instructions before connecting the system to the power source.

Circuit Breaker

- ⊗ **WARNING:** This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 250 V, 20 A.

Power Disconnection Warning

- ⊗ **WARNING:** The system must be disconnected from all sources of power and the power cord removed from the power supply module(s) before accessing the chassis interior to install or remove system components.

Equipment installation

- ⊗ **WARNING:** Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Restricted area

- ⊗ **WARNING:** This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. (This warning does not apply to workstations.)

Battery handling

- ⊗ **WARNING:** There is a danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Redundant power supplies

- ⊗ **WARNING:** This unit may have more than one power supply connection. All connections must be removed to de-energize the unit.

Backplane voltage

- ⊗ **WARNING:** Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.

Comply with local and national electrical codes

- ⊗ **WARNING:** Installation of equipment must comply with local and national electrical codes.

Product disposal

- ⊗ **WARNING:** Ultimate disposal of this product should be handled according to all national laws and regulations.

Hot swap fan warning

- ⊗ **WARNING:** The fans may still be turning when you remove the fan assembly from the chassis. Keep fingers, screwdrivers, and other objects away from the openings in the fan assembly's housing.

Power cable and AC adapter

- ⊗ **WARNING:** When installing the product, use the provided or designated connection cables, power cables, and AC adapters. Using any other cables and adapters can cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL or CSA-certified cables (which have UL/CSA shown on the code) for any other electrical devices than products designed by One Identity LLC only.

Virtual machine

Safeguard for Privileged Passwords can be run from:

- The One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance or 2000 Appliance (hardware)
- A virtual machine
- The cloud

This section covers the background and steps you need to set up the virtual machine for the first time.

[Using the virtual appliance and web management console](#)

[Setting up the virtual appliance](#)

[Support Kiosk](#)

[Virtual appliance backup and recovery](#)

Using the virtual appliance and web management console

Before you start: platforms and resources

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. See [One Identity's Product Support Policies](#) for more information on environment virtualization.

You must license the VM with a Microsoft Windows license. Specific questions about licensing should be directed to your Sales Representative.

Platforms and versions follow.




- You must license the VM with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed

to your Sales Representative.


- Supported hypervisors:
 - Microsoft Hyper-V (VHDX) version 8 or higher
 - VMware vSphere with vSphere Hypervisor (ESXi) versions 6.5 or higher
 - VMware Workstation version 13 or higher
- Minimum resources: 4 CPUs, 10GB RAM, and a 500GB disk. The virtual appliances default deploy does not provide adequate resources. Ensure these minimum resources are met.

Available wizards

The Appliance Administrator responsible for racking and initial configuration of the appliance can create the virtual appliance, launch the Safeguard web management console, and select one of the following wizards.

-  **Initial Setup:** Used to set up the virtual appliance for the first time including naming, OS licensing, and networking. For more information, see [Setting up the virtual appliance](#) on page 17.
-  **Setup:** After the first setup, Safeguard for Privileged Passwords updates and networking changes can be made via the web management console by clicking **Setup**.
-  **Support Kiosk:** The **Support Kiosk** is used to diagnose and resolve issues with Safeguard for Privileged Passwords. Any user able to access the kiosk can perform low-risk support operations including appliance restart or shutdown and support bundle creation. In order to reset the admin password, the user must obtain a challenge response token from One Identity support. For more information, see [Support Kiosk](#).

Security

 **CAUTION:** To maximize security in the absence of a hardened appliance, restrict the access to the Safeguard virtual disks, the web management console, and the MGMT interface to as few users as possible. The Management web kiosk gives access to functions without authentication, such as pulling a support bundle and rebooting the appliance.

Security recommendations follow.

- X0 hosts the public API and is network adapter 1 in the virtual machine settings. Connect this to your internal network.
- MGMT hosts the web management console and is network adapter 2 in the virtual machine settings. This interface always has the IP address of 192.168.1.105. Connect this to a private, restricted network accessible to administrators only, or disconnect it from the network to restrict unauthenticated actions such as rebooting or shutting down the appliance. The web management console is also available via the VMware console.

Once setup is completed, you can verify which of your NICs is MGMT and X0 by referring to the MAC address information found in **Support Kiosk > Appliance Information > Networking** for X0 and MGMT. For more information, see [Support Kiosk](#).

Backups: virtual appliance and hardware appliance

To protect the security posture of the Safeguard hardware appliance, Safeguard hardware appliances cannot be clustered with Safeguard virtual appliances. Backups taken from a hardware appliance cannot be restored on virtual appliances and backups taken from a virtual appliance cannot be restored on a hardware appliance.

For more information, see [Virtual appliance backup and recovery](#).

Upload and download

There is a web management console running on 192.168.1.105. When you connect to the virtual appliance via the virtual display, the web management console is displayed automatically; however, upload and download functionality are disabled when connected this way.

You may choose to configure the networking of your virtual machine infrastructure to enable you to proxy to <https://192.168.1.105> from your desktop. Connecting in this way will enable you to upload and download from the web management console.

⚠ CAUTION: Cloning and snapshotting are not supported and should not be used. Instead of cloning, deploy a new VM and perform Initial Setup. Instead of snapshotting, take a backup of the virtual appliance. Only the Safeguard for Privileged Passwords backup and recovery functionality is supported ([Virtual appliance backup and recovery](#)).

Migrating the VM

VMware VMotion can be used for live migration of a virtual machine from one physical server to another.

Setting up the virtual appliance

The Appliance Administrator uses the initial setup wizard to give the virtual appliance a unique identity, license the underlying operating system, and configure the network. The initial setup wizard only needs to be run one time after the virtual appliance is first deployed, but you may run it again in the future. It will not modify the appliance identity if run in the future.

Once set up, the Appliance Administrator can change the appliance name, license, and networking information, but not the appliance identity (ApplianceID). The appliance must have a unique identity.

The steps for the Appliance Administrator to initially set up the virtual appliance follow.

Step 1: Make adequate resources available

The virtual appliances default deploy does not provide adequate resources. The minimum resources required are: 4 CPUs, 10GB RAM, and a 500GB disk. Without adequate disk space, the patch will fail and you will need to expand disk space then re-upload the patch.

Step 2: Deploy the VM

Deploy the virtual machine (VM) to your virtual infrastructure. The virtual appliance is in the **InitialSetupRequired** state.

Hyper-V zip file import and set up

If you are using Hyper-V, you will need the Safeguard Hyper-V zip file distributed by One Identity to setup the virtual appliance. Follow these steps to unzip the file and import:

1. Unzip the Safeguard-hyperv-prod... zip file.
2. From Hyper-V, click **Options**.
3. Select **Action, Import Virtual Machine**.
4. On the **Locate Folder** tab, navigate to specify the folder containing the virtual machine to import then click **Select Folder**.
5. On the **Locate Folder** tab, click **Next**.
6. On the **Select Virtual Machine** tab, select Safeguard-hyperv-prod....
7. Click **Next**.
8. On the **Choose Import Type** tab, select **Copy the virtual machine (create a new unique ID)**.
9. Click **Next**.
10. On the **Choose Destination** tab, add the locations for the **Virtual machine configuration folder, Checkpoint store, and Smart Paging folder**.
11. Click **Next**.
12. On the Choose Storage Folders tab, identify **Where do you want to store the imported virtual hard disks for this virtual machine?**
13. Click **Next**.
14. Review the **Summary** tab, then click **Finish**.
15. In the **Settings, Add Hardware**, connect to Safeguard's MGMT and X0 network adapter.
16. Right-click on the Safeguard-hyperv-prod... and click **Connect...** to complete the configuration and connect.

Step 3: Initial access

Initiate access using one of these methods:


- Via a virtual display: Connect to the virtual display of the virtual machine. You will not be offered the opportunity to apply a patch with this access method. Upload and download are not available from the virtual display. Continue to step 3. If you are using Hyper-V, make sure that Enhanced Session Mode is disabled for the display. See your Hyper-V documentation for details.
- Via a browser: Configure the networking of your virtual infrastructure to proxy <https://192.168.1.105> on the virtual appliance to an address accessible from your workstation then open a browser to that address. For instructions on how to do this, consult the documentation of your virtual infrastructure (for example, VMWare). You will be offered the opportunity to apply a patch with this access method. Upload and download are available from the browser. Continue to step 3.

IMPORTANT: After importing the OVA and before powering it on, check the VM to make sure it doesn't have a USB controller. If there is a USB controller, remove it.

Step 4: Complete initial setup

Click **Begin Initial Setup**. Once this step is complete, the appliance resumes in the **Online** state.

Step 5: Log in and configure Safeguard for Privileged Passwords

1. If you are applying a patch, check your resources and expand the disk space, if necessary. The minimum resources are: 4 CPUs, 10GB RAM, and a 500GB disk.
2. To log in, enter the following default credentials for the Bootstrap Administrator then click **Log in**.
 - User Name: admin
 - Password: Admin123
3. If you are using a browser connected via <https://192.168.1.105>, the **Initial Setup** pane identifies the current Safeguard version and offers the opportunity to apply a patch. Click **Upload Patch** to upload the patch to the current Safeguard version or click **Skip**. (This is not available when using the Safeguard Virtual Kiosk virtual display.)
4. In the web management console on the  **Initial Setup** pane, enter the following.
 - a. **Appliance Name:** Enter the name of the virtual appliance.
 - b. **Host DNS Suffix:** Enter the host DNS suffix name.
 - c. **Windows Licensing:** Select one of the following options:
 - **Use KMS Server:** If you leave this field blank, Safeguard will use DNS to locate the KMS Server automatically. For the KMS Server to be found, you will need to have defined the domain name in the DNS Suffixes.

If KMS is not registered with DNS, enter the network IP address of your KMS server.

- **Use Product Key:** If selected, your appliance will need to be connected to the internet for the necessary verification to add your organization's Microsoft activation key.
- d. **NTP:** Complete the Network Time Protocol (NTP) configuration.
 - Select **Enable NTP** to enable the protocol.
 - Identify the **Primary NTP Server** IP address and, optionally, the **Secondary NTP Server** IP address.
 - e. **Network (X0):** For the X0 (public) interface, enter the IPv4 and/or IPv6 information, and **DNS Servers** information. Directory or network scans are supported for IPv4 but not IPv6.
5. Click **Save**. The virtual appliance displays progress information as it configures Safeguard, the network adapter(s), and the operating system licensing.
 6. When you see the message `Maintenance is complete`, click **Continue**.

Step 6: Access the web client

You can go to the virtual appliance's IP address for the X0 (public) interface from your browser.

Step 7: Change the Bootstrap Administrator's password



For security reasons, change the password on the Bootstrap Administrator User. For details, see the *Safeguard for Privileged Passwords Administration Guide*, Setting a local user's password.

Step 8. After clustering, change the trusted servers, CORS, and redirects setting

As a best practice, after you have created your Safeguard for Privileged Passwords cluster (or if just using a single VM), change the Trusted Servers, CORS and Redirects setting to the empty string or a list of values to integration applications you wish to allow. For more details, see the *Safeguard for Privileged Passwords Administration Guide*, Trusted Servers, CORS and Redirects.

View or change the virtual appliance setup

You can view or change the virtual appliance setup.

- From the web management console, click  **Home** to see the virtual appliance name, licensing, and networking information.
- After the first setup, Safeguard for Privileged Passwords updates and networking changes can be made via the web management console by clicking  **Setup**.

Support Kiosk

An Appliance Administrator triaging a Hyper-V or VMware virtual appliance that has lost connectivity or is otherwise impaired can use the Support Kiosk even when the virtual appliance is in quarantine. For more information, see *What do I do when an appliance goes into quarantine* in the *Safeguard for Privileged Passwords Administration Guide*.

It is recommended that terminal settings be 90 x 45 or larger. Smaller settings may result in an error like: `Screen dimension to small`.

When using the Windows Kiosk it is not possible to copy and paste. In Hyper-V it is possible to automate typing text from the keyboard, and using full ESX it may be possible to emulate keypresses via the API call `PutUsbScanCodes()`.

1. On the web management console, click  **Support Kiosk**.

2. Select any of the following activities:

- **Appliance Information**

This is read-only. You can re-run setup to change networking information.

- **Power Options**

You can reboot or shutdown the virtual appliance.

- a. Enter the reason you want to reboot or shutdown the virtual appliance.
- b. Click **Reboot** or **Shutdown**.

- **Admin Password Reset**

The Bootstrap Administrator is a built-in account to get the appliance running for the first time. The default credentials (admin/Admin123) should be changed once Safeguard is configured. If you lose the password, you can reset it to the default using the challenge response process below.

Challenge response process

- a. In **Full Name or Email**, enter your name or email to receive the challenge question.
- b. Click **Get Challenge**.
- c. To get the challenge response, perform one of the following (see the illustration that follows).
 - Click **Copy Challenge**. The challenge is copied to the clipboard. Send that challenge to Safeguard support. Support will send back a challenge response that is good for 48 hours. Do not refresh your

screen.

- Screenshot the QR code and send it to Support. Support will send back a challenge response that is good for 48 hours.

Do not navigate away from the page or refresh during a challenge response operation. Doing so will invalidate the challenge response and you will need to restart the process.

- Use a QR code reader on your phone to get the challenge response.

This action requires you get a challenge from the appliance, send it to Safeguard support, and enter the response provided.

Full Name or Email *

Andrew

Copy Challenge

Challenge QR Code



Enter the challenge response below.

Response *

d. After the response is accepted, click **Reset Password**. Once the operation has completed, the password for the admin account will be defaulted back to **Admin123**.

- **Support Bundle**

A support bundle includes system and configuration information sent to One Identity Support to analyze and diagnose issues. You can download a support bundle or save the bundle to a Windows share location which you have already set up. To generate a support bundle:

1. Select **Include Event Logs** if you want to include operating system events. Unless requested by support, it is recommended to leave this unchecked because it takes much longer to generate the support bundle.
2. Create the support bundle using one of these methods:
 - If you are connected via the browser not the display, you can click **Download**, navigate to the location for the download, and click **OK**.
 - To copy the bundle to the share:
 1. Enter the **UNC Path**, **Username**, and **Password**.
 2. Select **Include Event Logs**, if appropriate.

3. Click **Copy To Share**. A progress bar displays. The operation is complete when you see The bundle was successfully copied to the share.

- **Diagnostic package**

Appliance Administrators can execute a trusted, secure appliance diagnostics package to help solve issues with configuration, synchronization, and clustering, as well as other other internal challenges. The appliance diagnostics package is available from the web Support Kiosk, not the Serial Kiosk (Recovery Kiosk). The appliance diagnostics package can be used even when the appliance is in quarantine. To protect against external threats, Safeguard rejects illegitimate appliance diagnostics packages. The manifest file in the appliance diagnostics package lists criteria that may include the minimum Safeguard version, appliance ID, and expiration time-stamp UTC. New product code and database changes are not included in an appliance diagnostics package.

- a. To load for the first time, click **Upload**, select the file that has an .sgd extension, then click **Open**.
 - If the upload criteria is not met, the appliance diagnostics package is not uploaded and a message like the following displays: The minimum Safeguard version needed to run this diagnostic package is <version>.
 - If the upload is successful, the **Diagnostic Package Information** displays with a **Status** of **Staged**. Select **Execute** and wait until the **Status** changes to **Completed**.
- b. Once uploaded, you can:
 - Select **Download Log** to save the log file. Audit log entries are available through the Activity Center during and after execution and are part of the appliance history.
 - If the **Expiration Date** has not passed, you can select **Execute** to execute the appliance diagnostics package again.
 - Select **Delete** to delete the appliance diagnostics package, the associated log file, and stop any appliance diagnostics package that is running. Before uploading a different appliance diagnostics package, you must delete the current one because there can be only one appliance diagnostics package per appliance.

Virtual appliance backup and recovery

Use the following information to back up and recover a Safeguard for Privileged Passwords virtual appliance. Factory reset is not an option for virtual appliances. To factory reset a virtual appliance, just redeploy the appliance.

Backing up the virtual appliance

To ensure security of the hardware appliance, backups taken from a hardware appliance cannot be restored on virtual appliances and backups taken from a virtual appliance cannot be restored on a hardware appliance.

For more information, see Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Recovery of the virtual appliance

A Safeguard for Privileged Passwords virtual appliance is reset by using the following recovery steps.

On-prem virtual appliance (for example, Hyper-V or VMware)

1. Redeploy the virtual appliance and run **Initial Setup**. For more information, see Setting up the virtual appliance in the *Safeguard for Privileged Passwords Administration Guide*.
2. Restore the backup. For more information, see Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Cloud virtual appliance (for example, AWS or Azure)

1. Redeploy using the deployment steps:
 - AWS: For more information, see [AWS deployment](#).
 - Azure: For more information, see [Azure deployment](#).


Completing the appliance setup

After setting up the hardware appliance or virtual appliance, complete these steps.

Step 1: Log in to the web client

1. Log in using the Bootstrap Administrator account with the configured IPv4 or IPv6 address for the primary interface (X0). To log in with an IPv6 address, enter it in square brackets.
2. License Safeguard for Privileged Passwords using the provided license file. Go to **Licensing**:

-  (web client): **Appliance Management > Appliance > Licensing**.

Click  to upload a new license file.

The Software Transaction Agreement will be displayed after a new license is uploaded and must be read and accepted in order to use Safeguard for Privileged Passwords.


3. Defining archive server configurations and assigning an archive server to an appliance are done from **Appliance Management**:
 - Go to **Appliance Management > Backup and Retention > Archive Servers** to configure archive servers.
4. To configure the time zone:
 - a. Navigate to **User Management > Settings > Time Zone**.
 - b. Select the time zone in the **Default User Time Zone** drop-down menu.
5. Ensure that your Safeguard for Privileged Passwords Appliance has the latest software version installed. To check the version:
 - a. Click **Appliance Management > Appliance > Appliance Information**. The **Appliance Version** is displayed.
 - b. Go to the following product support page for the latest version:
<https://support.oneidentity.com/one-identity-safeguard/download-new-releases>
 - c. If necessary, apply a patch. Wait for maintenance to complete. If you are installing multiple patches, repeat as needed.

- i. Download the latest update from: <https://support.oneidentity.com/one-identity-safeguard/>.
- ii. From the Safeguard for Privileged Passwords Home page, select **Appliance Management > Appliance > Patch Updates**.
- iii. Click **Upload a File** and browse to select an update file.
NOTE: When you select a file, Safeguard for Privileged Passwords uploads it to the server, but does not install it.
- iv. Click **Install Now** to install the update file immediately.
- v. In the confirmation dialog, enter the word **Install** and click **OK**.
- vi. Once you have updated Safeguard for Privileged Passwords, be sure to back up your Safeguard for Privileged Passwords Appliance.

Changing the Bootstrap Administrator's password

The Bootstrap Administrator is a built-in account that allows you to get the appliance set up for first-time use. To keep your Safeguard for Privileged Passwords Appliance secure, once the license is added, change the default password for the Bootstrap Administrator's account.

To change the password (local users):

-  web client: Click your user name in the upper-right corner of the screen and select **My Settings**. Open the **My Account** page and click the **Change Password** button.

If this password is ever lost, you can reset it to the default of Admin123. See the *Safeguard for Privileged Passwords Administration Guide*, [Admin password reset](#) topic.

Step 2: Backup Safeguard for Privileged Passwords

Immediately after your initial installation of Safeguard for Privileged Passwords, make a backup of your Safeguard for Privileged Passwords Appliance.

NOTE: The default backup schedule runs at 4:00 AM UTC, which can be modified or you can manually run a backup.

1. From the Safeguard for Privileged Passwords Home page, open **Appliance Management > Backup and Retention > Backup and Restore**.
2. Click **+ Run Now**.

Step 3: Add a user with Authorizer administrative permissions

The Authorizer Administrator is responsible for granting administrative access to One Identity Safeguard for Privileged Passwords.

1. From the Safeguard for Privileged Passwords Home page, open **User Management > Users**.
2. Click **+ New User** to create a Safeguard for Privileged Passwords user with local identity and authentication, and Authorizer permissions.

NOTE: When you choose **Authorizer** permissions, Safeguard for Privileged Passwords also selects **User** and **Help Desk** permissions. These additional settings cannot be cleared.

3. Log out:
 - a. In the upper-right corner of the screen, click your user name.
 - b. Select **Log Out**.

Cloud deployments

Safeguard for Privileged Passwords can be run from:

- The One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance or 2000 Appliance (hardware)
- A virtual machine
- The cloud

This section covers the background and steps you need to deploy from the cloud for the first time.

[Cloud deployment considerations](#)

[AWS deployment](#)

[Azure deployment](#)

[Virtual appliance backup and recovery](#)

Cloud deployment considerations

Safeguard for Privileged Passwords can be run from the cloud.

Before you start: platforms and resources

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. See [One Identity's Product Support Policies](#) for more information on environment virtualization.

Platforms that have been tested with the cloud deployments follow.

- AWS Virtual Machine (VM): For more information, see [AWS deployment](#) on page 30.
- Azure Virtual Machine (VM): For more information, see [Azure deployment](#) on page 32.

For these deployments, the minimum resources used in test are 4 CPUs, 10GB RAM, and a 60GB disk. Choose the appropriate machine and configuration template. For example,

when you click **Create** in the Azure Marketplace, default profiles display. You can click **Change size** to choose a different template.

Restricting access to the web management kiosk for cloud deployments

The web management kiosk runs on port 9337 in AWS and Azure and is intended for diagnostics and troubleshooting by Appliance Administrators.

⚠ CAUTION: The Management web kiosk is available via HTTPS port 9337 for cloud platforms (including AWS and Azure). The Management web kiosk gives access to functions without authentication, such as pulling a support bundle or rebooting the appliance. In AWS, all ports are denied unless explicitly allowed. To deny access to port 9337, the port should be left out of the firewall rules. If the port is used, firewall rules should allow access to targeted users.

Azure: Block port 9337

Use the following steps to block access to port 9337 in Azure.

1. Navigate to the virtual machine running Safeguard for Privileged Passwords.
2. In the left hand navigation menu select **Networking**.
3. Click **Add inbound port rule**.
4. Configure the inbound security rule as follows:
Source: Any
Source port ranges: *
Destination: Any
Destination port ranges: 9337
Protocol: Any
Action: Deny
Priority: 100 (use the lowest priority for this rule)
Name: DenyPort9337
5. Click **Add**.

AWS: Block port 9337

Use the following steps to block access to port 9337 in AWS.

1. From the EC2 Dashboard, navigate to the EC2 Instance running Safeguard for Privileged Passwords.
2. Select the instance.
3. In the **Description** tab, locate the **Security groups** field then click the name of the security group.
4. Select the **Inbound** tab.
5. Click **Edit**.
6. Remove any existing rules and add the following rules:
 - Type: Custom UDP Rule
Protocol: UDP

Port Range: 655
Source: Anywhere
Description: Cluster VPN

- Type: HTTPS
Protocol: TCP
Port range: 443
Source: Anywhere
Description: Web API
- Type: Custom TCP Rule
Protocol: TCP
Port Range: 8649
Source: Anywhere
Description: SPS Cluster

7. Click **Save**.

AWS deployment

IMPORTANT: Before deploying, make sure you have read [Cloud deployment considerations](#)

Safeguard for Privileged Passwords (SPP) can be run in the cloud using Amazon Web Services (AWS).

To deploy the Amazon Machine Image (AMI) of Safeguard for Privileged Passwords from AWS, visit the AWS marketplace listing for Safeguard for Privileged Passwords ([here](#)) and follow the [Deployment steps](#).

Disk size considerations

CAUTION: Before making any changes to the disk size, shut down the VM (stopped and deallocated).

Safeguard for Privileged Passwords (SPP) deploys with a minimal OS disk size. You should increase the size of the OS disk based on your estimated usage and budget. SPP on hardware comes with 1TB of disk. You can use more or less than this depending on how many assets, accounts, and daily users you expect to have. 500GB is a minimal production disk size and 2TB is the maximum.

Disk size can be handled through Amazon Elastic Compute Cloud (Amazon EC2). For more information, see [Getting Started with Amazon EC2](#). When you start up the VM, SPP automatically resizes the OS disk volume to use the available space.

AWS security considerations

Running Safeguard for Privileged Passwords (SPP) in AWS comes with some security considerations that do not apply to the hardware appliance. We recommend:

- Do not give Safeguard a public IP address.
- Use the AWS key vault to encrypt the disk.
- Limit access within AWS to the Safeguard virtual machine. SPP in AWS cannot protect against rogue Administrators in the same way the hardware appliance can.

Static IP address required

Configure the SPP VM with a static IP address in AWS. In AWS, the IP address must not change after the VM is deployed. If you need to change the IP address, take a backup, deploy again, and restore the backup. You can script the VM deploy to pick up an existing virtual NIC with the IP address configuration. For details, see the [Amazon Virtual Private Cloud \(VPC\)](#) documentation.

Deployment steps

AWS automatically licenses the operating system during the deployment with an AWS KMS. Larger deployments warrant larger sizing choices. Safeguard for Privileged Passwords hardware appliances have 32GB of RAM and 4 processors with at least 1TB of disk space.

AWS Marketplace steps

1. Go to the AWS marketplace listing for Safeguard for Privileged Passwords ([here](#)).
2. On the One Identity Safeguard for Privileged Passwords page, click **Continue to Subscribe**.
3. Advance through the resource creation screens to configure your instance. In addition to the [Disk size considerations](#), [AWS security considerations](#), and [Static IP address required](#); One Identity recommends you select the **m4.2xlarge** instance type.
4. Once you have finished configuring the instance, select to launch the instance.

| **NOTE:** The instance launch process may take a while to complete.

5. Once the instance has finished launching, log into the web client using your static IP address. You will need to use the default username (**admin**) and password (**<instance id>**). You should change the admin password immediately. For details, see the *Safeguard for Privileged Passwords Administration Guide*, Setting a local user's password.

| **NOTE:** The password is unique for each deployment and the initial password will always be the instance ID of the deployed safeguard server.

View or change the cloud virtual appliance setup

You can view or change the virtual appliance setup.

You can use the Safeguard for Privileged Passwords web management kiosk on port 9337 for diagnostics and troubleshooting.

You can also check the system logs via AWS:

1. To view the system log from AWS, select **Actions**, then **Instance Settings**, and then **Get System Log**.
2. Log in via `https://<your IP>:9337`

To patch to a new version, use the API.

Azure deployment

IMPORTANT: Before deploying, make sure you have read [Cloud deployment considerations](#)

Safeguard for Privileged Passwords (SPP) can be run in the cloud using Azure. A version of Safeguard for Privileged Passwords is available in the Azure Marketplace and an Azure Virtual Machine (VM) is required. See [Windows virtual machines in Azure](#) for details of setting up your VM.

When using Azure, Safeguard for Privileged Passwords is available on HTTPS X0. The Azure deployment does not use the MGMT service. The Recovery (Serial) Kiosk is used to view appliance information, Administrator password reset, power restart or shut down, and generating a support bundle. For more information, see Recovery Kiosk (Serial Kiosk) in the *Safeguard for Privileged Passwords Administration Guide*.

Disk size considerations

Safeguard for Privileged Passwords (SPP) deploys with a minimal OS disk size. You should increase the size of the OS disk based on your estimated usage and budget. SPP on hardware comes with 1TB of disk. You can use more or less than this depending on how many assets, accounts, and daily users you expect to have. 500GB is a minimal production disk size and 2TB is the maximum.

1. Deploy SPP.
2. Verify you can log in.
3. Shut down the VM (stopped and deallocated).
4. Follow Microsoft's guidance for increasing the disk size: [How to expand the OS drive of a virtual machine](#).

When you start up the VM, SPP automatically resizes the OS disk volume to use the available space.

Azure security considerations

Running Safeguard for Privileged Passwords (SPP) in Azure comes with some security considerations that do not apply to the hardware appliance. We recommend:

- Do not give Safeguard a public IP address.
- Use the Azure key vault to encrypt the disk.

- Limit access within Azure to the Safeguard virtual machine. SPP in Azure cannot protect against rogue Administrators in the same way the hardware appliance can.

Static IP address recommended

Configure the SPP VM with a static IP address in Azure. In Azure, the IP address must not change after the VM is deployed. If you need to change the IP address, take a backup, deploy again, and restore the backup. You can script the VM deploy to pick up an existing virtual NIC with the IP address configuration. For details, see Microsoft's [Virtual Network](#) documentation.

Deployment steps

Safeguard for Privileged Passwords is deployed from the Azure Marketplace. Azure automatically licenses the operating system during the deployment with an Azure KMS.

The Azure base image includes the required configuration necessary to deploy into Azure following Microsoft's guidance, [Prepare a Windows VHD or VHDX to upload to Azure](#).

1. Log into the Azure portal.
2. Under **Azure services**, click **Create a resource**.
3. Search for "One Identity Safeguard for Privileged Passwords" and click the tile.
4. On the One Identity Safeguard for Privileged Passwords screen, click **Create**.
5. Advance through the resource creation screens. Considerations follow:
 - For small deployments, it is recommended to choose at least VM size Standard D2s v3. Larger deployments warrant larger sizing choices. Safeguard hardware appliances have 32GB of RAM and 4 processors with at least 1 TB of disk space.
 - You must set an administrator user name and password as part of the image creation, however, SPP will disable this account during initial setup.
 - Set public inbound ports to **None**.
 - Choose your Windows licensing option.
 - Make sure to enable boot diagnostics and the serial kiosk. The Azure Serial console will be used to provide access to the Safeguard Recovery Kiosk.
6. Once you are finished configuring the VM, click **Create**. Azure will deploy the SPP virtual machine.
7. When the virtual machine deployment is finished, SPP will automatically start initializing and configuring itself for the first use. This usually takes between 5-30 minutes, depending on the VM sizing. During initialization, Safeguard will enable the firewall and disable remote access to the VM. You can monitor the progress of initialization from the Azure Serial console. While the initialization is running, do not log in to the VM or power off or restart the VM.
8. When initialization is complete, you will see the Safeguard Recovery (Serial) Kiosk on the Azure Serial console screen.
9. Log in to the appliance via the web using the default username and password admin / Admin123. You should change the admin password immediately. For details, see the

Safeguard for Privileged Passwords Administration Guide, Setting a local user's password.

10. After clustering, change the trusted servers, CORS and redirects setting. As a best practice, after you have created your Safeguard for Privileged Passwords cluster (or if just using a single VM), change the Trusted Servers, CORS and Redirects setting to the empty string or a list of values to integration applications you wish to allow. For more details, see the *Safeguard for Privileged Passwords Administration Guide*, Trusted Servers, CORS and Redirects.

View or change the cloud virtual appliance setup

You can view or change the virtual appliance setup.

The Administrator uses the Recovery Kiosk (Serial Kiosk) to perform the following.

- Get appliance information
- Reset the Administrator password
- Restart or shut down the virtual appliance
- Generate a support bundle
- Resolve a quarantine (for more information, see What do I do when an appliance goes into quarantine in the *Safeguard for Privileged Passwords Administration Guide*).

For more information, see Recovery Kiosk (Serial Kiosk) in the *Safeguard for Privileged Passwords Administration Guide*.

To patch to a new version, use the API.

Virtual appliance backup and recovery

Use the following information to back up and recover a Safeguard for Privileged Passwords virtual appliance. Factory reset is not an option for virtual appliances. To factory reset a virtual appliance, just redeploy the appliance.

Backing up the virtual appliance

To ensure security of the hardware appliance, backups taken from a hardware appliance cannot be restored on virtual appliances and backups taken from a virtual appliance cannot be restored on a hardware appliance.

For more information, see Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Recovery of the virtual appliance

A Safeguard for Privileged Passwords virtual appliance is reset by using the following recovery steps.

On-prem virtual appliance (for example, Hyper-V or VMware)

1. Redeploy the virtual appliance and run **Initial Setup**. For more information, see Setting up the virtual appliance in the *Safeguard for Privileged Passwords Administration Guide*.
2. Restore the backup. For more information, see Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Cloud virtual appliance (for example, AWS or Azure)

1. Redeploy using the deployment steps:
 - AWS: For more information, see [AWS deployment](#).
 - Azure: For more information, see [Azure deployment](#).

System requirements and versions

One Identity Safeguard for Privileged Passwords allows you to manage access requests, approvals, and reviews for your managed accounts and systems.

- The web client consists of an end-user view and administrator view. The fully featured client exposes all of the functionality of Safeguard based on the role of the authenticated user.
- The web management console displays whenever you connect to the virtual appliance and is used for first time configuration. 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. See [One Identity's Product Support Policies](#) for more information on environment virtualization.

Ensure that your system meets the minimum hardware and software requirements for these clients.

If a Safeguard Sessions Appliance is linked to Safeguard for Privileged Passwords, session recording is handled via Safeguard for Privileged Session. The link is initiated from Safeguard for Privileged Sessions. For details about the link steps and issue resolution, see the [One Identity Safeguard for Privileged Sessions Administration Guide](#).

Bandwidth

It is recommended that connection, including overhead, is faster than 10 megabits per second inter-site bandwidth with a one-way latency of less than 500 milliseconds. If you are using traffic shaping, you must allow sufficient bandwidth and priority to port 655 UDP in the shaping profile. These numbers are offered as a guideline only in that other factors could require additional network tuning. These factors include but are not limited to: jitter, packet loss, response time, usage, and network saturation. If there are any further questions, please check with your Network Administration team.

Web client system requirements

Table 1: Web requirements

Component	Requirements
Web browsers	<p>Desktop browsers:</p> <ul style="list-style-type: none">• Apple Safari 16.0 for desktop (or later)• Google Chrome 108 (or later)• Microsoft Edge 108 (or later)• Mozilla Firefox 108 (or later) <p>Mobile device browsers:</p> <ul style="list-style-type: none">• Apple Safari Mobile 14.7 (or later)• Google Chrome on Android 108 (or later)

Web management console system requirements

Table 2: Web kiosk requirements

Component	Requirements
Web management console	<p>Desktop browsers:</p> <ul style="list-style-type: none">• Apple Safari 16.0 for desktop (or later)• Google Chrome 108 (or later)• Microsoft Edge 108 (or later)• Mozilla Firefox 108 (or later)

Platforms and versions follow.

- You must license the VM with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative.
- Supported hypervisors:
 - Microsoft Hyper-V (VHDX) version 8 or higher
 - VMware vSphere with vSphere Hypervisor (ESXi) versions 6.5 or higher
 - VMware Workstation version 13 or higher

- Minimum resources: 4 CPUs, 10GB RAM, and a 500GB disk. The virtual appliances default deploy does not provide adequate resources. Ensure these minimum resources are met.

Supported platforms

One Identity Safeguard for Privileged Passwords supports a variety of platforms, including custom platforms.

Safeguard for Privileged Passwords tested platforms

The following table lists the platforms and versions that have been tested for Safeguard for Privileged Passwords (SPP). Additional assets may be added to Safeguard for Privileged Passwords. If you do not see a particular platform listed when adding an asset, use the **Other**, **Other Managed**, **Other Directory**, or **Linux** selection on the **Management** tab of the **Asset** dialog.

SPP linked to SPS: Sessions platforms

CAUTION: When linking your One Identity Safeguard for Privileged Sessions (SPS) deployment to your One Identity Safeguard for Privileged Passwords (SPP) deployment, ensure that the SPS and SPP versions match exactly, and keep the versions synchronized during an upgrade. For example, you can only link SPS version 6.6 to SPP version 6.6, and if you upgrade SPS to version 6.7, you must also upgrade SPP to 6.7.

Make sure that you do not mix Long Term Supported (LTS) and feature releases. For example, do not link an SPS version 6.0.1 to an SPP version 6.1.

When Safeguard for Privileged Passwords (SPP) is linked with a Safeguard for Privileged Sessions (SPS) appliance, platforms are supported that use one of these protocols:

- SPP 2.8 or lower: RDP, SSH
- SPP 2.9 or higher: RDP, SSH, or Telnet

Some platforms may support more than one protocol. For example, a Linux (or Linux variation) platform supports both SSH and Telnet protocols.

Table 3: Supported platforms: Assets that can be managed

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
ACF2 - Mainframe	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
ACF2 - Mainframe LDAP	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	False
Active Directory	Active Directory	True	False
AIX	AIX 7.2 AIX 7.3	True	True
Amazon Linux	Amazon Linux 2 Amazon Linux 2022 Amazon Linux Other	True	True
Amazon Web Services	Amazon Web Services 1	True	False
CentOS Linux	CentOS Linux 7 CentOS Linux 8	True	True
Check Point GAIa (SSH)	Check Point GAIa (SSH) R80.30 Check Point GAIa (SSH) R81	True	True
Cisco ASA	Cisco ASA 7.X Cisco ASA 8.X Cisco ASA 9.X	True	True
Cisco IOS (510)	Cisco IOS 12.X Cisco IOS 15.X Cisco IOS 16.X	True	True
Cisco ISE	Cisco ISE 2.7 Cisco ISE 3	True	False
Cisco ISE CLI	Cisco ISE CLI 2.7 Cisco ISE CLI 3	True	True
Cisco NX-OS	Cisco NX-OS 9.3(7) Cisco NX-OS 9.3(7a)	True	True
Debian GNU/Linux	Debian GNU/Linux 10 Debian GNU/Linux 11 Debian GNU/Linux 12	True	True
Dell iDRAC	Dell iDRAC 8	True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
	Dell iDRAC 9		
eDirectory LDAP	eDirectory LDAP 9.0	True	False
ESXi	ESXi 7.0 ESXi 8.0	True	False
F5 Big-IP	F5 Big-IP 12.1.2 F5 Big-IP 13.0 F5 Big-IP 14.0 F5 Big-IP 15.0	True	True
Fedora	Fedora 37 Fedora 38	True	True
Fortinet FortiOS	Fortinet FortiOS 6.2 Fortinet FortiOS 6.4 Fortinet FortiOS 7.0 Fortinet FortiOS 7.2	True	True
FreeBSD	FreeBSD 12 FreeBSD 13	True	True
HP iLO	HP iLO 4 HP iLO 5 HP iLO 6	True	True
HP iLO MP	HP iLO MP 2 HP iLO MP 3	True	True
HP-UX	HP-UX 11iv3 (B.11.31)	True	True
IBM i	IBM i 7.3 IBM i 7.4	True	True
Junos - Juniper Networks	Junos - Juniper Networks 19 Junos - Juniper Networks 20 Junos - Juniper Networks 21 Junos - Juniper Networks 22	True	True
LDAP	OpenLDAP 2.4	True	False
Linux		True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
macOS	macOS 11 macOS 12 macOS 13	True	True
MongoDB	MongoDB 4.4 MongoDB 5.0 MongoDB 6.0	True	False
MySQL	MySQL 5.7 MySQL 8.0 MySQL 8.1	True	False
Oracle	Oracle 19c Oracle 21c	True	False
Oracle Linux (OL)	Oracle Linux (OL) 7 Oracle Linux (OL) 8 Oracle Linux (OL) 9	True	True
Other		False	False
Other Directory		True	False
Other Managed		True	False
PAN-OS	PAN-OS 9.1 PAN-OS 10.1 PAN-OS 10.2	True	True
PostgreSQL	PostgreSQL 11 PostgreSQL 12 PostgreSQL 13 PostgreSQL 14 PostgreSQL 15	True	False
RACF - Mainframe	RACF - Mainframe z/OS V2.1 Security Server zSeries RACF - Mainframe z/OS V2.2 Security Server zSeries RACF - Mainframe z/OS V2.3 Security Server zSeries	True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
RACF - RACF - Mainframe LDAP	RACF - Mainframe LDAP z/OS V2.1 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.2 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.3 Security Server zSeries	True	False
Red Hat Enterprise Linux (RHEL)	Red Hat Enterprise Linux (RHEL) 7 Red Hat Enterprise Linux (RHEL) 8 Red Hat Enterprise Linux (RHEL) 9	True	True
Red Hat Directory Server	Red Hat Directory Server 11 Red Hat Directory Server 12	True	False
SAP HANA	SAP HANA SAP HANA 2	True	False
SAP Netweaver Application Server	SAP Netweaver Application Server 7.5	True	False
Solaris	Solaris 10 Solaris 11.3 Solaris 11.4	True	True
SonicOS	SonicOS 6.5 SonicOS 7 SonicOSX 7	True	False
SonicWALL SMA or CMS	SonicWALL SMA or CMS 11.3.0	True	False
SQL Server	SQL Server 2014 SQL Server 2016 SQL Server 2017 SQL Server 2019 SQL Server 2022	True	False
SUSE Linux Enterprise Server (SLES)	SUSE Linux Enterprise Server (SLES) 12 SUSE Linux Enterprise Server (SLES) 15	True	True
Sybase (Adaptive)	Sybase (Adaptive Server Enterprise)	True	False

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
Server Enterprise)	15.7 Sybase (Adaptive Server Enterprise) 16 Sybase (Adaptive Server Enterprise) 17		
Top Secret - Mainframe	Top Secret - Mainframe r14 zSeries Top Secret - Mainframe r15 zSeries Top Secret - Mainframe r16 zSeries	True	False
Top Secret - Mainframe LDAP	Top Secret - Mainframe LDAP r14 Top Secret - Mainframe LDAP r15 Top Secret - Mainframe LDAP r16	True	True
Ubuntu	Ubuntu 18.04 LTS Ubuntu 22.04 LTS Ubuntu 22.10	True	True
Windows Desktop	Windows (SSH) 10	True	True
Windows Desktop (SSH)	Windows (SSH) 11 Windows (SSH) Server 2012		
Windows Desktop (WinRM)	Windows (SSH) Server 2012 R2		
Windows Server	Windows (SSH) Server 2016		
Windows Server (SSH)	Windows (SSH) Server 2019 Windows (SSH) Server 2022		
Windows Server (WinRM)	Windows 10 Windows 11 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022		

Table 4: Supported platforms: Directories that can be searched

Platform Name	Platform Version
Microsoft Active Directory	Windows 2008+ DFL/FFL
LDAP	2.4

For all supported platforms, it is assumed that you are applying the latest updates. For unpatched versions of supported platforms, Support will investigate and assist on a case-by-case basis but it may be necessary for you to upgrade the platform or use SPP's custom platform feature.

Custom platforms

The following example platform scripts are available:

- Custom HTTP
- Linux SSH
- Telnet
- TN3270 transports are available

For more information, see *Custom Platforms and Creating a custom platform script* in the *Safeguard for Privileged Passwords Administration Guide*.

Sample custom platform scripts and command details are available at the following links available from the [Safeguard Custom Platform Home](#) wiki on GitHub:

- Command-Reference:
<https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Command-Reference>
- Writing a custom platform script:
<https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/WritingACustomPlatformScript>
- Example platform scripts are available at this location:
<https://github.com/OneIdentity/SafeguardCustomPlatform/tree/master/SampleScripts>

⚠ CAUTION: Example scripts are provided for information only. Updates, error checking, and testing are required before using them in production. Safeguard for Privileged Passwords checks to ensure the values match the type of the property that include a string, boolean, integer, or password (which is called secret in the API scripts). Safeguard for Privileged Passwords cannot check the validity or system impact of values entered for custom platforms.

Licenses

Hardware appliance

The One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance ship with the Privileged Passwords module which requires a valid license to

enable functionality.

You must install a valid license. Once the module is installed, Safeguard for Privileged Passwords shows a license state of **Licensed** and is operational. If the module license is not installed, you have limited functionality. That is, even though you will be able to configure access requests, if a Privileged Passwords module license is not installed, you will not be able to request a password release.

Virtual appliance Microsoft Windows licensing

You must license the virtual appliance with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative. The virtual appliance will not function unless the operating system is properly licensed.

Licensing setup and update

To enter licensing information when you first log in

The first time you log in as the Appliance Administrator, you are prompted to add a license. The **Success** dialog displays when the license is added.

On the virtual appliance, the license is added as part of Initial Setup.

IMPORTANT: After successfully adding a license, the Software Transaction Agreement will be displayed and must be read and accepted in order to use Safeguard for Privileged Passwords.

To configure reminders for license expiration

To avoid disruptions in the use of Safeguard for Privileged Passwords, the Appliance Administrator must configure the SMTP server, and define email templates for the License Expired and the License Expiring Soon event types. This ensures you will be notified of an approaching expiration date.

Users are instructed to contact their Appliance Administrator if they get an "appliance is unlicensed" notification.

As an Appliance Administrator, if you receive a "license expiring" notification, apply a new license.


To update the licensing file

Licensing update is only available using a virtual machine, not via the hardware.

To perform licensing activities

Go to the licensing page:

1. Navigate to **Appliance > Licensing**.
 - To upload a new license file, click **+Upload new license file** and browse to select the current license file. The Software Transaction Agreement will also be displayed during this process and must be read and accepted in order to complete the licensing process.

- To remove the license file, select the license and click  **Remove selected license.**

Long Term Support (LTS) and Feature Releases

Releases use the following version designations:


- Long Term Support (LTS) Releases: The first digit identifies the release and the second is a zero (for example, 6.0 LTS).
- Maintenance LTS Releases: A third digit is added followed by LTS (for example, 6.0.6 LTS).
- Feature Releases: The Feature Releases version numbers are two digits (for example, 6.6).

Customers choose between two paths for receiving releases: Long Term Support (LTS) Release or Feature Release. See the following table for details.

Table 5: Comparison of Long Term Support (LTS) Release and Feature Release

	Long Term Support (LTS) Release	Feature Release
General Release	<p>Scope: Includes new features, resolved issues and security updates</p> <p>Versioning: The first digit identifies the LTS and the second digit is a 0 (for example, 6.0 LTS, 7.0 LTS, and so on).</p>	<p>Scope: Includes the latest features, resolved issues, and other updates, such as security patches for the OS</p> <p>Versioning: The first digit identifies the LTS and the second digit is a number identifying the Feature Release (for example, 6.6, 6.7, and so on).</p>
Maintenance Release	<p>Scope: Includes critical resolved issues</p> <p>Versioning: A third digit designates the maintenance LTS Release (for example, 6.0.6 LTS).</p>	<p>Scope: Includes highly critical resolved issues</p> <p>Versioning: A third digit designates the maintenance Feature Release (for example, 6.6.1).</p>

Release and support details can be found at [Product Life Cycle](#).

 **CAUTION: Downgrading from the latest Feature Release, even to an LTS release, voids support for SPP.**

One Identity strongly recommends always installing the latest revision of the release path you use (Long Term Support path or Feature Release path).

Moving between LTS and Feature Release versions

You can move from an LTS version (for example, 6.0.7 LTS) to the same feature version (6.7) and then patch to a later feature version. After that, you can patch from the minimum version for the patch, typically N-3. If you move from an LTS version to a feature version, you will receive a warning like the following which informs you that you will only be able to apply a Feature Release until the next LTS Release:

Warning: You are patching to a Feature Release from an LTS Release. If you apply this update, you will not be able to upgrade to a non-Feature Release until the next LTS major release version is available. See the Administration Guide for details.

You cannot move from a Feature Release to LTS Release. For example, you cannot move from 6.7 to 6.0.7 LTS. You have to keep upgrading with each new Feature Release until the next LTS Release version is published. For this example, you would wait until 7.0 LTS is available.

Patching

You can only patch from a major version. For example, if you have version 6.6 and want to patch to 7.7, you must patch to 7.0 LTS and then apply 7.7.

An LTS major version of Safeguard for Privileged Passwords (SPP) will only work with the same LTS major version of Safeguard for Privileged Sessions (SPS). For the best experience, it is recommended you use the latest supported version.

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