One Identity Safeguard for Privileged Passwords 2.11.1

Appliance Setup Guide

Safeguard for Privileged Passwords Appliance Setup Guide
Updated - April 2020
Version - 2.11.1

Contents

Hardware appliance

Safeguard for Privileged Passwords can be run from:

- The One Identity Safeguard for Privileged Passwords 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

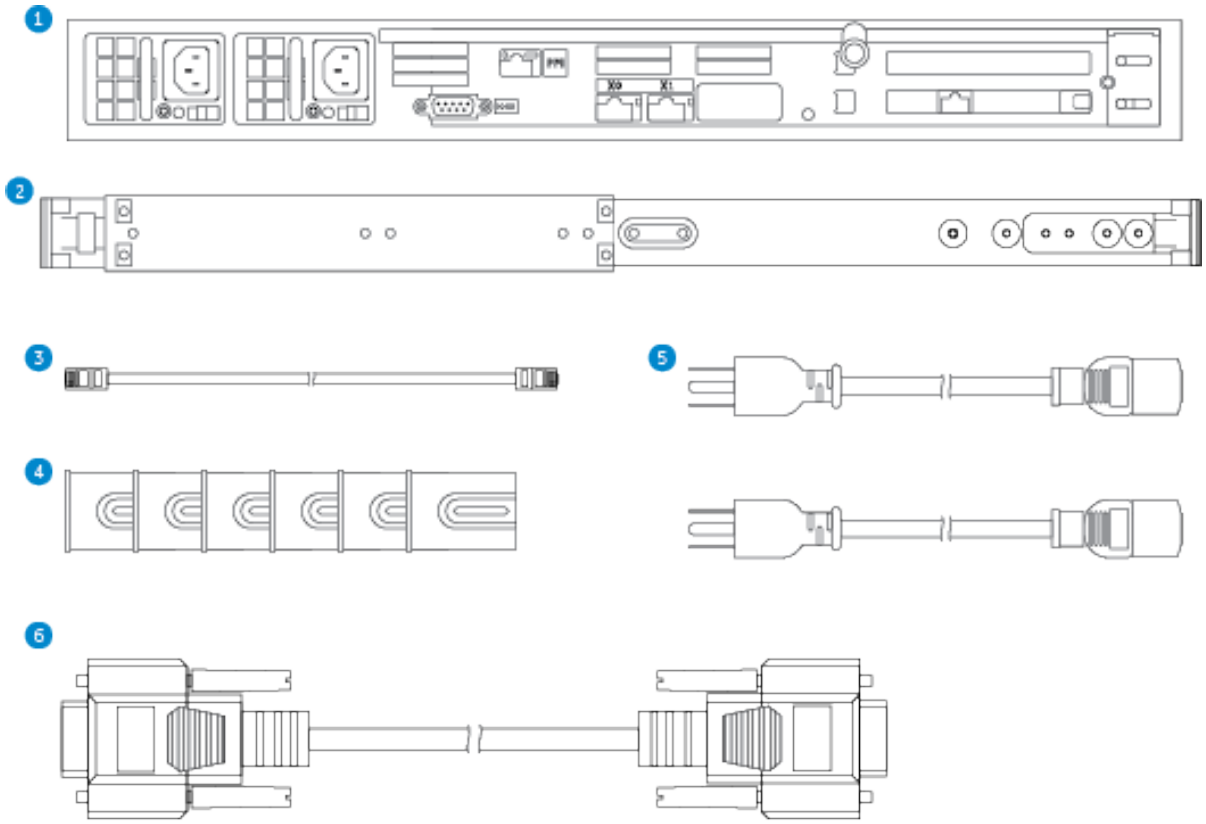
In addition to this guide, the One Identity Safeguard for Privileged Passwords package contents includes the following as shown in the figure below:

1. One Identity Safeguard for Privileged Passwords 2000 Appliance
2. Rail (2)
3. Ethernet cable
4. Extra rail installation brackets
5. Power cord (2)*
6. 6-foot DB9F/DB9F serial cable

*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

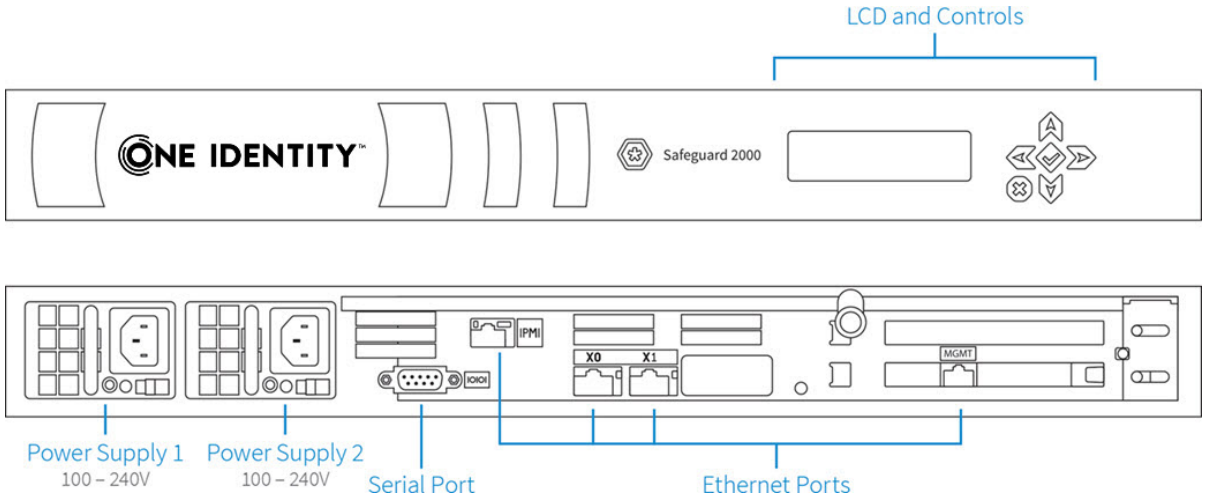
Figure 1: Package contents



Front and back panels

The following diagram shows the front and back panels on the One Identity Safeguard for Privileged Passwords 2000 Appliance.

Figure 2: Front and back panels



Operating conditions and regulatory compliance

Operating conditions (運行條件)

Input (輸入/输入):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.

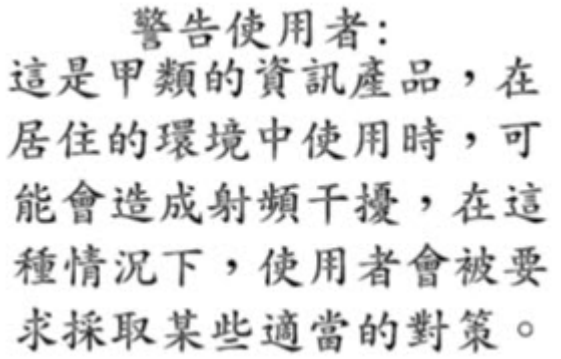
VCCI warning

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

Follow these steps to set up and configure the One Identity Safeguard for Privileged Passwords 2000 Appliance.

Step 1: Before you start

Ensure that you install the Microsoft .NET Framework 4.6 (or later) on your management host.

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

  If a Safeguard for Privileged Passwords Appliance is going to be used for both Privileged Passwords and the sessions module, you need this network interface information for both the appliance and the embedded sessions module.

  CAUTION:The embedded sessions module in Safeguard for Privileged Passwords version 2.7 (and later) will be removed in a future release (to be determined). For uninterrupted service, organizations are advised to join to the more robust Safeguard for Privileged Sessions Appliance for sessions recording and playback.

  - 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.

    Safeguard for Privileged Passwords ships with the following modules, each requiring a valid license to enable functionality:

    - Privileged passwords
    - Embedded sessions module

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 2000 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**
4. 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.
   - To change the password from the web client, click **Settings** in the upper-right corner of the screen and select **Change Password**.
   - 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.
5. Configure the primary network interface (X0):
   a. 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)
        - Enter the DNS server address.
        - Optional, enter the DNS suffixes.
        - Click **Save**.

   NOTE: The **Network Interface (X1)** information must be configured to use the embedded sessions module. You can configure the **Network Interface (X1)** for the Privileged Sessions module now or later using the Windows desktop client or web client.

> If one or more Safeguard Sessions Appliances are joined to Safeguard for Privileged Passwords, X1 is not available in Safeguard for Privileged Passwords.

Step 7: Connect the appliance to the network

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

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 14.
- 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 (Tmra).

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 2000 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.

2

Virtual machine

Safeguard for Privileged Passwords can be run from:

- The One Identity Safeguard for Privileged Passwords 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

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 and versions that have been tested with the web management console follow.

- Operating system: Windows 10 Enterprise LTSC including dynamic disks. If you are using KMS, the KMS server needs to be able to validate Windows 10 Enterprise LTSC.

- Supported VMs:
  - Microsoft Hyper-V (VHDX) version 8 or higher
  - VMware vSphere with vSphere Hypervisor (ESXi) version 6.5 or higher
  - VMWare Workstation version 6.5 or higher
- Minimum resources recommended: 4 CPUs, 10GB RAM, and a 500GB disk

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 19.
- **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 on page 22.

Security

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.

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 on page 22.

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.

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: 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...`, then click **Next**.
7. On the **Choose Import Type** tab, select **Copy the virtual machine (create a new unique ID)**, then click **Next**.
8. On the **Choose Destination** tab, add the locations for the **Virtual machine configuration folder**, **Checkpoint store**, and **Smart Paging folder**, then click **Next**.
9. On the Choose Storage Folders tab, identify **Where do you want to store the imported virtual hard disks for this virtual machine?** then click **Next**.
10. Review the **Summary** tab, then click **Finish**.
11. In the **Settings**, **Add Hardware**, connect to Safeguard's MGMT and X0 network adapter.
12. Right click on the `Safeguard-hyperv-prod...` and click **Connect...** to complete the configuration and connect.

Step 2: 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 3: Complete initial setup

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

Step 4: Log in and configure Safeguard for Privileged Passwords

1. To log in, enter the following default credentials for the Bootstrap Administrator then click **Log in**.
    - User Name: admin
    - Password: Admin123
2. 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.)
3. In the web management console on the **Initial Setup** pane, enter the following.
    a. **Appliance Name**: Enter the name of the virtual appliance.
    b. **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.

          You can update this information in **Administrative Tools** | **Settings** | **Appliance** | **Operating System Licensing**. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Operating system license.
    c. **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.
    d. **Network (X0)**: For the X0 (public) interface, enter the IPv4 and/or IPv6 information, and **DNS Servers** information.
4. Click **Save**. The virtual appliance displays progress information as it configures Safeguard, the network adapter(s), and the operating system licensing.
5. When you see the message `Maintenance is complete`, click **Continue**.

Step 5: Access the desktop client or use the web client

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

- Use the web client. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Using the web client.
- Log in and download the desktop client. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Installing the desktop client.

Step 6: 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.

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 the *Safeguard for Privileged Passwords Administration Guide*, What do I do when an appliance goes into quarantine.

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.

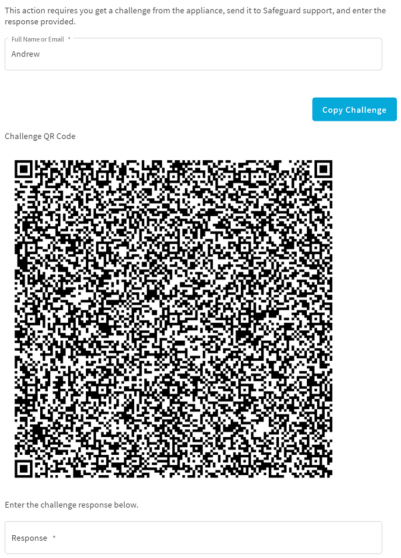
Challenge response process

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



d. After the response is accepted, click **Reset Password**.

- **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.

- **Factory Reset** (hardware appliance)

  A virtual appliance is reset by the recovery steps to redeploy and not a factory reset. If you are attached to the console of a virtual machine, you will not have the Factory Reset option. The options are only available for hardware. Perform a factory reset to recover from major problems or to clear the data

and configuration settings on a hardware appliance. All data and audit history is lost and the hardware appliance goes into maintenance mode. For more information, see Performing a factory reset.

- **Lights Out Managment (BMC)** (hardware appliance)
  The Lights Out Management feature allows you to remotely manage the power state and serial console to Safeguard for Privileged Passwords using the baseboard management controller (BMC). When a LAN interface is configured, this allows the Appliance Administrator to power on an appliance remotely or to interact with the Recovery Kiosk.
  For more information, see Lights Out Management (BMC).

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.

Backup is handled via **Administrative Tools** | **Settings** | **Backup and Retention**. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Backup and retention settings.

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 on page 19.
2. Restore the backup. For more information, see Backup and Retention settings. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Backup and retention settings.

Cloud virtual appliance (for example, Azure)

1. Redeploy using the deployment steps:
   - Azure: For more information, see Using Azure on page 27.

3

Cloud deployment

Safeguard for Privileged Passwords can be run from:

- The One Identity Safeguard for Privileged Passwords 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.

Using the cloud

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.

- Azure Virtual Machine (VM): For more information, see Using Azure on page 27.

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 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 Azure). The Management web kiosk gives access to functions without authentication, such as pulling a support bundle or rebooting the appliance.**

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**.

Using Azure

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).

Disk size considerations

Safeguard for Privileged Passwords (SPP) deploys with a minimal OS disk size, typically 30GB. 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. Currently, a minimum of 60GB is required for patching up.

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.

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.)

For more information, see Recovery Kiosk (Serial Kiosk).

To patch to a new version, use the desktop client or 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.

Backup is handled via **Administrative Tools** | **Settings** | **Backup and Retention**. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Backup and retention settings.

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 on page 19.
2. Restore the backup. For more information, see Backup and Retention settings. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Backup and retention settings.

Cloud virtual appliance (for example, Azure)

1. Redeploy using the deployment steps:
    - Azure: For more information, see Using Azure on page 27.

Completing the appliance setup

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

Step 1: Install the desktop client application and desktop player

NOTE: PuTTY is used to launch the SSH client for SSH session requests and is included in the install. The desktop client looks for any user-installed PuTTY in the following locations:

- Any reference to putty in the PATH environment variable
- `c:/Program Files/Putty`
- `c:/Program Files(x86)/Putty`
- `c:/Putty`

If PuTTY is not found, the desktop client uses the version of PuTTY that it installed at:

`<user-home-dir>/AppData/Local/Safeguard/putty`.

If the user later installs PuTTY in any of the locations above, the desktop client uses that version which ensures the user has the latest version of PuTTY.

Installing the Safeguard for Privileged Passwords desktop client application

1. To download the Safeguard for Privileged Passwords desktop client Windows installer .msi file, open a browser and navigate to:

   https://<Appliance IP>/Safeguard.msi

   Save the **Safeguard.msi** file in a location of your choice.
2. Run the MSI package.
3. Select **Next** in the **Welcome** dialog.
4. Accept the **End-User License Agreement** and select **Next**.
5. Select **Install** to begin the installation.
6. Select **Finish** to exit the desktop client setup wizard.

Installing the Desktop Player

> **CAUTION: If the Desktop Player is not installed and a user tries to play back a session from the Activity Center, a message like the following will display:** `No Desktop Player. The Safeguard Desktop Player is not installed. Would you like to install it now?` **The user will need to click Yes to go to the download page to install the player following step 2 below.**

1. Once the Safeguard for Privileged Passwords installation is complete, go to the Windows **Start** menu, **Safeguard** folder, and click **Download Safeguard Player** to be taken to the One Identity Safeguard for Privileged Sessions - Download Software web page.
2. Follow the *Install Safeguard Desktop Player* section of the player user guide found here:
    a. Go to One Identity Safeguard for Privileged Sessions - Technical Documentation.
    b. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.
3. For Safeguard Desktop player version 1.8.6 and later, ensure your signed web certificate has a Subject Alternative Name (SAN) that includes each IP address of each of your cluster members. If the settings are not correct, the Safeguard Desktop Player will generate a certificate warning like the following when replaying sessions: `Unable to verify SSL certificate. To resolve this issue, import the appropriate certificates including the root CA.`

New Desktop Player versions

When you have installed a version of the Safeguard Desktop Player application, you will need to uninstall the previous version to upgrade to a newer player version.

Step 2: Start the desktop client

1. Log in using the Bootstrap Administrator account.
2. Run the desktop client and log in with the configured IPv4 or IPv6 address for the primary interface (X0). To log in with an IPv6 address, enter it in square brackets.
3. License one or both of the Safeguard for Privileged Passwords modules using the provided license files:
    - Privileged passwords
    - Embedded sessions module
4. Designate an archive server for storing session recordings. Defining archive server configurations and assigning an archive server to an appliance are done from the desktop's **Administrative Tools** view:
    - Go to **Settings** | **Backup and Retention** | **Archive Servers** to configure archive servers.
    - Go to **Settings** | **Sessions** | **Session Recordings Storage Management** to assign an archive server to an appliance for storing recording files.

5. To configure the time zone:
    a. Navigate to **Administrative Tools** | **Settings** | **Safeguard Access** | **Time Zone**.
    b. Select the time zone in the **Default User Time Zone** drop-down menu.
6. Ensure that your Safeguard for Privileged Passwords Appliance has the latest software version installed. To check the version:
    a. From the Safeguard for Privileged Passwords Desktop Client, log in with admin account credentials.
    b. Click **Settings** | **Appliance** | **Appliance Information**. The **Appliance Version** is displayed.
    c. Go to the following product support page for the latest version:

    https://support.oneidentity.com/one-identity-safeguard/download-new-releases
    d. If necessary, apply a patch. Wait for maintenance. If you are installing multiple patches, repeat as needed.

Step 3: 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 22:00 MST, which can be modified rather than manually running a backup.

1. From the Safeguard for Privileged Passwords desktop Home page, select **Administrative Tools**.
2. In **Settings**, select **Backup and Retention** | **Backups**.
3. Click **+ Run Now**.

Step 4: Update Safeguard for Privileged Passwords

Download the latest update from: https://support.oneidentity.com/one-identity-safeguard/.

1. From the Safeguard for Privileged Passwords desktop Home page, select **Administrative Tools**.
2. In **Settings**, select **Appliance** | **Updates**.
3. 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.
4. Click **Install Now** to install the update file immediately.
5. Once you have updated Safeguard for Privileged Passwords, be sure to back up your Safeguard for Privileged Passwords Appliance.

Step 5: 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 desktop Home page, select **Administrative Tools**.

   NOTE: This is where you add all the objects you need to write access request policies, such as users, accounts, and assets.

2. In **Administrative Tools**, select **Users**.
3. Click **+ Add User** to create a Safeguard for Privileged Passwords user with a local authentication provider and Authorizer Administrator permissions.

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

4. Log out:

   a. In the upper-right corner of the screen, click the user avatar.

   b. Select **Log Out**.

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.