One Identity Safeguard for Privileged Passwords

Appliance Setup Guide

Legend

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

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

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

Safeguard for Privileged Passwords Appliance Setup Guide
Updated - May 2019

Contents

One Identity Safeguard for Privileged Passwords 2000 Appliance

This chapter provides a list of the main components included in the package and a description of the main features of the One Identity Safeguard for Privileged Passwords 2000 Appliance. It also describes the operating conditions and regulatory compliance.

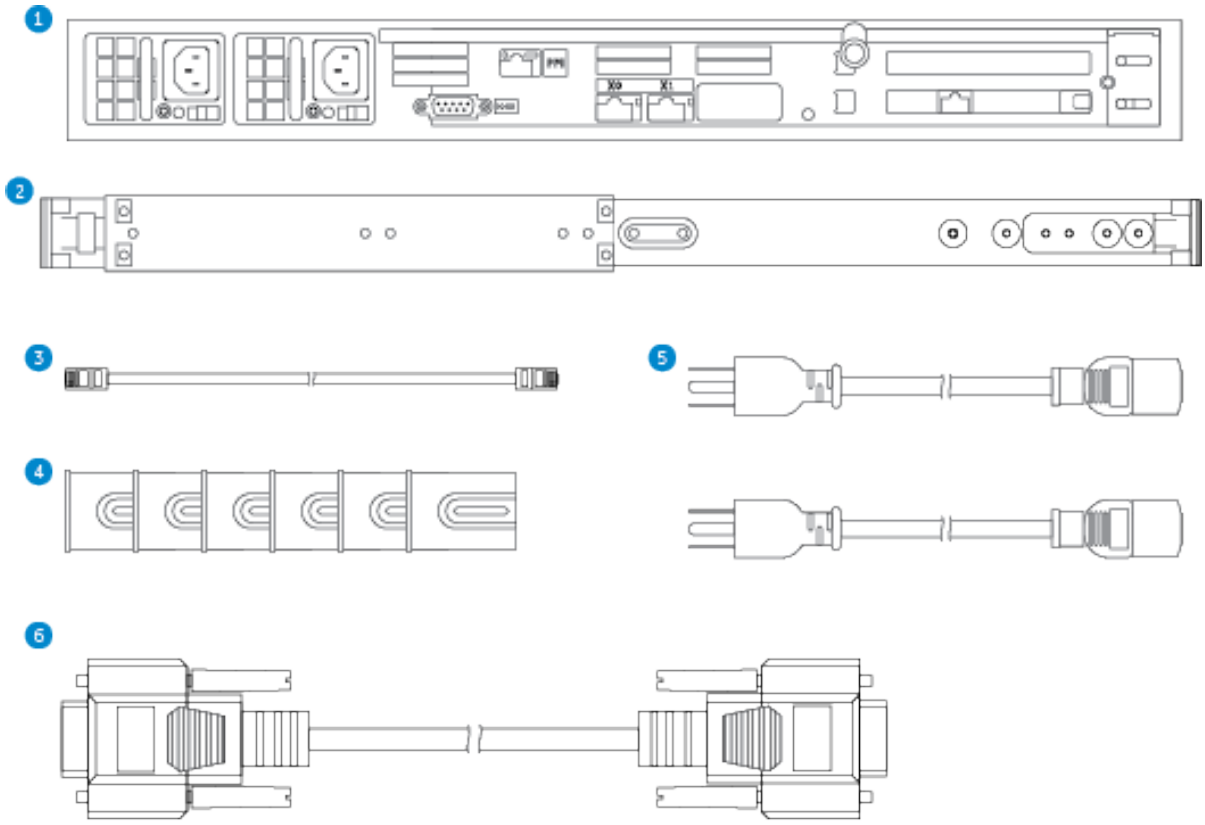
Package contents

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

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

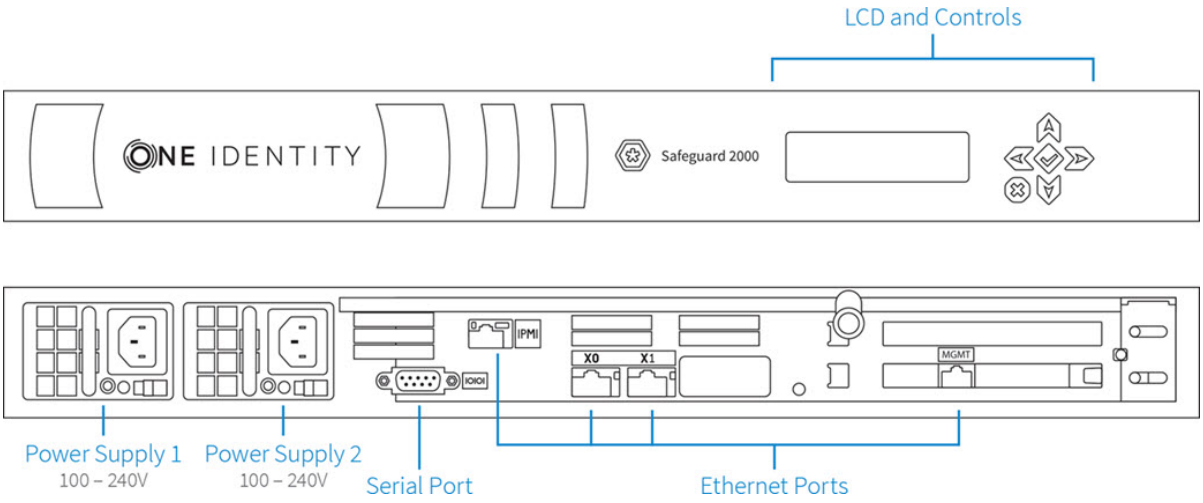
* The included power cords are approved by use only in specific countries or regions. Before using a power cord, verify that it is rated and approved for use in your location. The power cord is for AC mains installation only.

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



Front and back panels

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


LCD and Controls
ONE IDENTITY
Safeguard 2000
IPMI
X0
X1
MGMT
Power Supply 1
100 – 240V
Power Supply 2
100 – 240V
Serial Port
Ethernet Ports

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.

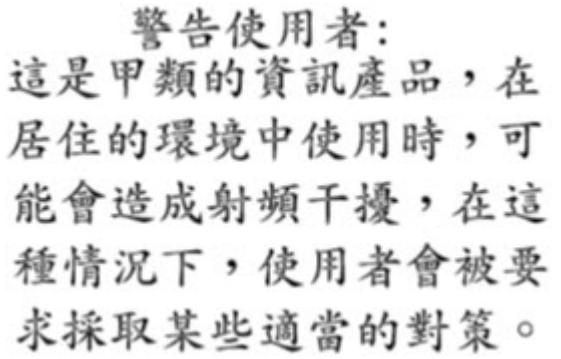
VCCI warning

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.



2

Setting up the appliance

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

Step 1: Before you start

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

Step 2: Prepare for installation

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

1. Laptop
2. IP address
3. IP subnet mask
4. IP gateway
5. DNS server address
6. NTP server address

   NOTE: 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 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.

7. 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.

NOTE: One Identity 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.

IMPORTANT: 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 into 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 into the Safeguard for Privileged Passwords Web client using the bootstrap administrator account:
   - User name: ***admin***
   - Password: ***Admin123***

     IMPORTANT: 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**.
4. 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.

Step 8: Configure Safeguard for Privileged Passwords

NOTE: When you install the Windows desktop client, the following is also installed:

- Safeguard for Privileged Passwords PuTTY which is used to launch the SSH client for SSH session requests.

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. Click this link: 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*.

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.

Starting the desktop client

1. Log in using the bootstrap administrator account from Step 6: Log into Safeguard for Privileged Passwords.
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 9: 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 10: 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 backup your Safeguard for Privileged Passwords Appliance.

Step 11: 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**.

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 18.
- 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 which 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 might 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 might 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 could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL or CSA -certified cables (that have UL/CSA shown on the code) for any other electrical devices than products designed by One Identity LLC only.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

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

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at: www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product