One Identity Safeguard for Privileged Sessions 5.8

Security Checklist

Legend

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

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

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

SPS Security Checklist
Updated - August 2018
Version - 5.8

Contents

3

Security checklist for configuring SPS

The following checklist is a set of recommendations and configuration best practices to ensure that your SPS is configured securely.

Encryption-related settings

- One Identity recommends using 2048-bit RSA keys (or stronger).
- Use strong passwords: at least 8 characters that include numbers, letters, special characters, and capital letters. For local SPS users, require the use of strong passwords (set **AAA > Settings > Minimal password strength** to `strong`). For details, see "Setting password policies for local users" in the Administration Guide.
- When exporting the configuration of SPS, or creating configuration backups, always use encryption. Handle the exported data with care, as it contains sensitive information, including credentials. For details on encrypting the configuration, see "Encrypting configuration backups with GPG" in the Administration Guide.
- Use every keypair or certificate only for one purpose. Do not reuse cryptographic keys or certificates, for example, do not use the certificate of the SPS webserver to encrypt audit trails, or do not use the same keypair for signing and encrypting data.
- Do not use the CBC block cipher mode, or the `diffie-hellman-group1-sha1` key exchange algorithm. For details, see "Supported encryption algorithms" in the Administration Guide.
- Always encrypt your audit trails to protect sensitive data. For details, see "Encrypting audit trails" in the Administration Guide.

Connection policies

- When configuring connection policies, always limit the source of the connection to the client network that requires access to the connection.
- Always use gateway authentication to authenticate clients. Do not trust the source IP address of a connection, or the result of server authentication.
- To prevent Denial of Service (DoS) attacks against SPS, set the **Connection rate limit** option of your connection policies. For details, see "Displaying custom connection statistics" in the Administration Guide.
- Configure your RDP connection policies to use strong encryption. To enable SSL-encryption for the RDP protocol, see "Enabling TLS-encryption for RDP connections" in the Administration Guide.
- In RDP connections, if the client uses the Windows login screen to authenticate on the server, the password of the client is visible in the audit trail. To avoid displaying the password when replaying the audit trail, you are recommended to encrypt the upstream traffic in the audit trail using a separate certificate from the downstream traffic. For details, see "Encrypting audit trails" in the Administration Guide.
- Ensure that host key verification is enabled in SSH connection policies. That is, the **Server side hostkey settings > Allow plain host keys** and **Server side hostkey settings > Allow X.509 host certificates** options do not have the **No check required** option selected. For details, see "Setting the SSH host keys and certificates of the connection" in the Administration Guide.

Appliance access

- Accessing the SPS host directly using SSH is not recommended or supported, except for troubleshooting purposes. In such case, the One Identity Support Team will give you exact instructions on what to do to solve the problem.

  For security reasons, disable SSH access to SPS when it is not needed. For details, see "Enabling SSH access to the SPS host" in the Administration Guide.
- Permit administrative access to SPS only from trusted networks. If possible, monitored connections and administrative access to the SPS web interface should originate from separate networks.
- Configure SPS to send an alert if a user fails to login to SPS. For details, see the **Login failed** alert in "System related traps" in the Administration Guide.
- Configure **Disk space fill-up prevention**, and configure SPS to send an alert if the free space on the disks of SPS is low. For details, see "Preventing disk space fill-up" in the Administration Guide.

Networking considerations

- SPS stores sensitive data. Use a firewall and other appropriate controls to ensure that unauthorized connections cannot access it.
- If possible, enable management access to SPS only from trusted networks.
- Make sure that the HA interface of SPS is connected to a trusted network.

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