One Identity Safeguard for Privileged Sessions 6.9

Common Criteria Evaluated Configuration Guide (CCECG)

Version 1.1

January 26, 2022

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

Table of Contents

Referenced Documentation

[3000UM] *Super SC113 Chassis Series User's Manual,* Version 1.0d, September 22, 2020 (The user guide for installing the Safeguard Sessions Appliance 3000.)

https://www.supermicro.com/manuals/chassis/1U/SC113.pdf

[3500UM] *Supermicro SuperServer 1029U-T Series User's Manual,* Revision 1.0i, September 22, 2020 (The user guide for installing the Safeguard Sessions Appliance 3500.)

https://www.supermicro.com/manuals/superserver/1U/MNL-1973.pdf

[Admin] *One Identity Safeguard for Privileged Sessions 6.9.3 Administration Guide*, Version 6.9.3, 30 April 2021

https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-sessions/6.9.3/administration-guide

[INSTAL] *One Identity Safeguard for Privileged Sessions Installation Guide*, Version 6.9.3, April 30, 2021

https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-sessions/6.9.3/installation-guide

[IPMI] *Supermicro BMC IPMI User's Guide, Revision 1.1b, August 26, 2020* (The user guide for the IPMI port on the SPS.)

https://www.supermicro.com/manuals/other/IPMI_Users_Guide.pdf

[PACK] *One Identity Safeguard for Privileged Sessions 6.9 Packaging Checklist*, Version 6.9.3, April 20, 2021

https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-sessions/6.9.3/packaging-checklist

[REST] *One Identity Safeguard for Privileged Sessions 6.9.3 REST API Reference Guide*, Version 6.9.3, April 30, 2021

https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-sessions/6.9.3/rest-api-reference-guide

[Upgrade] *One Identity Safeguard for Privileged Sessions 6.9.3 Upgrade Guide*, Version 6.9.3, April 30, 2021

https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-sessions/6.9.3/upgrade-guide

About This Guide

This guide is intended for administrators responsible for installing, configuring, and/or operating One Identity Safeguard for Privileged Sessions version 6.9 in accordance with the Common Criteria evaluation and the *collaborative Protection Profile for Network Devices, Version 2.2e* ([NDcPP]).

Guidance provided in this document allows you to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the Common Criteria evaluation.

You are expected to be familiar with the Security Target for One Identity Safeguard for Privileged Sessions 6.9 ([ST]) and the general Common Criteria terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target and provides instructions for how to perform the security functions that are defined by these SFRs.

The term "Administrator" used in this document refers generically to any user that has sufficient privileges to perform the activity being referenced.

The following table identifies the SFRs claimed by the product, a summary of the purpose of each SFR, and any administrative activities that are required to ensure the SFR is implemented correctly.

Table 1 SFR Summary

Requirement Name	Purpose of Requirement	Includes Guidance On
FAU_GEN.1	Generation of audit records for security-relevant events	Content and formatting of audit records for security-relevant events.
FAU_GEN.2	User identification in audit records	N/A; this requirement expects all audit events associated with user actions to log the user responsible for causing the event; this is automatically captured by the relevant audit records.
FAU_STG_EXT.1	Configuration of local and remote audit storage	Configuring an external syslog server to send audit records to and configuring local storage to mitigate the risk of disk space exhaustion.
FCS_CKM.1 & FCS_CKM.2	Cryptographic key generation and establishment	Configuring key generation and key establishment functions to use the algorithms that were certified in the evaluated configuration.
FCS_CKM.4	Cryptographic key destruction	Deleting persistently stored keys.
FCS_COP.1/Data Encryption	Data encryption	Configuring encryption functions to use the algorithms that were certified in the evaluated configuration.
FCS_COP.1/SigGen	Digital signature generation and verification	Configuring signature functions to use the algorithms that were certified in the evaluated configuration.
FCS_COP.1/Hash	Hash algorithms	Configuring hash functions to use the algorithms that were certified in the evaluated configuration.

Requirement Name	Purpose of Requirement	Includes Guidance On
FCS_COP.1/KeyedHash	Keyed hash algorithms	Configuring keyed hash functions to use the algorithms that were certified in the evaluated configuration.
FCS_HTTPS_EXT.1	HTTPS protocol implementation	Configuring the SPS HTTPS server interface.
FCS_RBG_EXT.1	Random bit generation	N/A; this requirement expects that a certain random bit generation algorithm is used, but this is enabled by default and is not configurable.
FCS_SSHC_EXT.1 and FCS_SSHS_EXT.1	SSH protocol implementation (as client and server)	Configuring the SSH client and server implementation to use the parameters that were certified in the evaluated configuration.
FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1	TLS protocol implementation (as client and server)	Configuring the TLS client and server implementation to use the parameters that were certified in the evaluated configuration.
FCS_TLSC_EXT.2	TLS client support for mutual authentication	Enabling SPS to support mutual authentication as a TLS client.
FIA_AFL.1	Product behavior following excessive failed authentication attempts	Configuring failed authentication lockout behavior and unlocking users that have been locked out due to excessive authentication failures.
FIA_PMG_EXT.1	Password policy management	Configuring the user password policy.
FIA_UAU_EXT.2 and FIA_UIA_EXT.1	User identification and authentication	Configuring administrator authentication mechanisms and authenticating to the management interfaces.
FIA_UAU.7	Nondisclosure of credential data in authentication feedback	N/A; this requirement expects that user credentials are obfuscated during input and failed login events, but this is enabled by default and is not configurable.
FIA_X509_EXT.1/Rev	X.509 certificate validation	Configuring X.509 trust stores and revocation behavior.
FIA_X509_EXT.2	The use of X.509 in support of authentication	N/A; this requirement relates to how X.509 certificates are used in support of authentication, but the relevant discussion is included in FIA_X509_EXT.1/Rev.
FIA_X509_EXT.3	X.509 certificate requests	Generating certificate signing requests and loading TLS client/server certificates onto the product.
FMT_MOF.1/ManualUpdate	Manual software update	Updating the product software/firmware.

Requirement Name	Purpose of Requirement	Includes Guidance On
FMT_MTD.1/CoreData	Management of configuration data	N/A; this requirement relates to the product's security-relevant management functionality, which is discussed under FMT_SMF.1 below.
FMT_MTD.1/CryptoKeys	Management of cryptographic keys	Performing operations against persistent keys used by the product (e.g. generate, import, modify, delete).
FMT_SMF.1	Summary of management functions	Performing the various security-relevant management functions that are claimed by the product.
FMT_SMR.2	Management roles	How administrators access the claimed management interface, and how administrative privileges are assigned to accounts.
FPT_APW_EXT.1	Secure credential storage	N/A; this requirement expects that user credential data is stored in a non-plaintext format, but this is enabled by default and is not configurable.
FPT_SKP_EXT.1	Secure key storage	Ensuring that there is no potential for plaintext key data to be exported from the product.
FPT_STM_EXT.1	System time data	Configuring the system clock.
FPT_TST_EXT.1	Self-testing	Product self-tests, how to detect when one has failed, and what to do in the event of such a failure.
FPT_TUD_EXT.1	Trusted update	N/A; this requirement covers product update behavior, which is covered by FMT_MOF.1/ManualUpdate above.
FTA_SSL_EXT.1 and FTA_SSL.3	System-initiated termination of user sessions	Configuring idle session timeout lengths.
FTA_SSL.4	User-initiated termination of user sessions	Manually terminating an active administrator session.
FTA_TAB.1	Administrator-specified advisory notice	Configuring the pre-authentication warning banner.
FTP_ITC.1	Secure communication with remote IT entities	Enabling the use of trusted communications protocols with external entities that support them.
FTP_TRP.1/Admin	Secure communication with remote users	Enabling the use of trusted communications protocols for remote administration.

Scope of the Evaluation

Safeguard for Privileged Sessions (SPS) is a network appliance that is able to enforce access control, authorization, and accounting methods on application-layer protocols that are commonly associated with management activities. The Common Criteria evaluated version is SPS version 6.9 running on the following hardware devices in a standalone configuration:

- Model 3000 with Intel Xeon E3-1275 CPU and
- Model 3500 with 2 x Intel Xeon Silver 4110 CPU

Other product deployments (e.g. virtual appliances, cloud appliances, high availability configuration) are outside the evaluation scope.

Not all of the product functionality is within the scope of the Common Criteria evaluation. The evaluated portion of SPS is referred to as the TOE (Target of Evaluation). The evaluated configuration is the TOE configured in such a manner to ensure that its security functionality is consistent with the claims made in its Security Target. This document identifies the configuration settings needed to ensure that the TOE is set up in its evaluated configuration. In the evaluated configuration, the TOE is responsible for secure proxying of SSH connections that carry application-layer protocols; the access control functionality for application-layer protocols is out of scope of the evaluation. Specifically, the TOE is responsible for ensuring the security of its own use and for the proper implementation of the secure communications protocols used for communication to, from, and through it.

The focus of this evaluation is on the TOE functionality supporting the claims in the collaborative Protection Profile for Network Devices ([NDcPP]). The security functionality specified in the [NDcPP] includes protection of communications between the TOE and external IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and use of NIST-validated cryptographic mechanisms.

Operational Environment Components

The TOE in its evaluated configuration requires the following components in its operational environment:

- A TLS-protected syslog server that receives audit events from the TOE;
- (optionally) an external LDAP/AD Server for authentication;
- at least one SSH client and at least one SSH server for session proxying using SSH. And
- a client workstation for administrator access to the system with:
  - A supported operating system: Windows 2008 Server, Windows 7, Windows 2012 Server, Windows 2012 R2 Server, Windows 8, Windows 8.1, Windows 10, Windows 2016, or any recent version of Linux. The OS must have the ability to run fairly recent versions of the admin clients (e.g. SSH) and a recent browser.
  - A supported browser: current version of Mozilla Firefox, current version of Google Chrome, Microsoft Edge, and Microsoft Internet Explorer 11 or newer. The browser must support TLS-encrypted HTTPS connections, and JavaScript/cookies must be enabled.
  - An external interface that is compatible with a serial port connector (for local console access).

The following diagram displays the TOE in an operational environment.

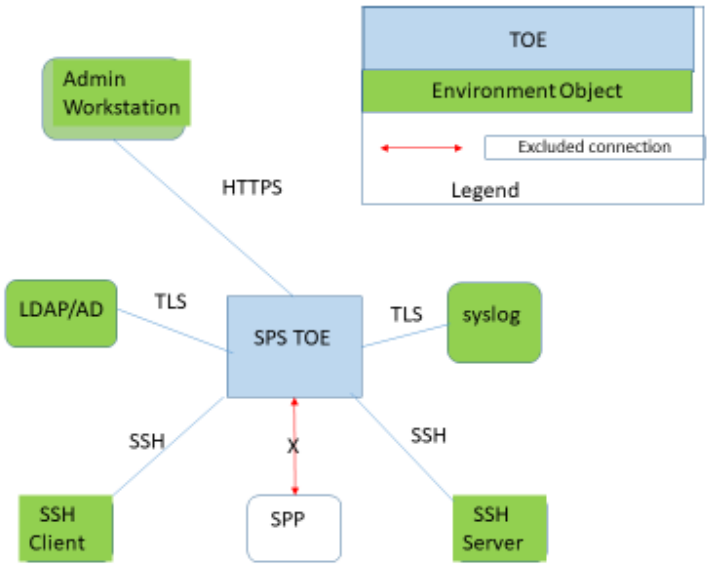

Figure 1: TOE in Operational Environment

Evaluation Assumptions

This section describes the assumptions made in identification of the threats and security requirements for Network Devices. The Network Device is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated. The following assumptions were made in performing the Common Criteria evaluation.

Table 2 Assumptions

Assumption	Guidance
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious

Assumption	Guidance
	intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Security Warnings

The following warnings apply generally to use of the system and should be adhered to in order to ensure secure use of the system:

- IPMI/BMC interfaces are only used during initial startup; when the product is in operational use this should only be accessible locally by an administrator for troubleshooting purposes. This interface should not be connected to an untrusted or externally accessible WAN.
- Protocol-level logging has a configurable option for how verbose the logs are. The default value is 4 and the range of allowed values is from 1-10. A value above 7 should not be used except for temporary troubleshooting purposes as this may cause sensitive data to be logged.
- The system is rendered inoperable if disk space is exhausted; reference the “Preventing disk space fill-up” section of [Admin] for preventative measures that can be taken to avoid this situation.
- Up to 10 MB or seven days of syslog data is retained locally; if an external syslog server becomes unavailable, the issue must be resolved promptly to mitigate the risk of audit data loss.
- If configuration data is being exported, it is necessary to ensure that the option to use encryption is chosen as the system configuration may include sensitive information.

Product Support

The One Identity product support page is located at https://support.oneidentity.com/one-identity-safeguard-for-privileged-sessions/. This page includes security bulletins, product documentation, and support contacts for product troubleshooting.

Initial Configuration

This section provides an overview of the initial steps of unpacking, assembling, and initially configuring the One Identity Safeguard for Privileged Sessions 6.9 (SPS). Refer to the referenced documentation for complete guidance.

Note the following:

- The product relies on OpenSSL 1.1.1 for cryptographic functions. The cryptographic algorithms used by the product in its evaluated configuration have been validated by the NIST Cryptographic Algorithm Validation Program; no special configuration is required to select or enable this cryptographic engine. Configuration instructions found the Cryptographic Support (FCS) section of this document describe how to limit cryptographic parameters to those that are within the scope the evaluation and have been certified. Use of any other cryptographic parameters is outside the scope of the evaluated configuration.
- The product includes an SSH interface, but completion of the Welcome Wizard will automatically disable it as part of first-time setup. This should not be re-enabled for the product to remain in its evaluated configuration.
- The product includes an IPMI interface. This interface is present on a dedicated management port and should only be used on a protected internal network if it is used at all. The use of IPMI is not required for any of the product functionality in the evaluated configuration and it is therefore recommended that it be disabled.
- The product includes several default user accounts with default credentials; as part of the initial installation process, these credentials must be changed. These are noted in the setup steps below.

1. Unpack SPS

   The shipment includes but is not limited to the following items.

   - The SPS appliance, pre-installed with One Identity Safeguard for Privileged Sessions firmware.
   - A copy of the *One Identity Safeguard for Privileged Sessions 6.9.3 Packaging Checklist* ([PACK]).
   - A GPL v2.0 license.
   - The default BIOS and IPMI passwords.

2. Install and Setup SPS

   Refer to *One Identity Safeguard for Privileged Sessions 6.9.3 Packaging Checklist* ([PACK]) included in with the shipment for guidance about setting up the One Identity SPS. The document includes guidance on setting up and installing a single SPS unit and describes but is not limited to the following items:

   - Install the appliance.
     - Refer to *Super SC113 Chassis Series User's Manual* ([3000UM]) for detailed guidance of installing the 3000 appliance.
     - Refer to *Supermicro SuperServer 1029U-T Series User's Manual* ([3500UM]) for detailed guidance about installing the 3500 appliance.
   - Connect the Ethernet cable to the LAN.

- Connect an Ethernet cable to the IPMI interface of SPS and connect to the IPMI remote console. For details refer to *Super X9 SMT IPMI User's Guide* ([IPMI]) for detailed guidance.
- Configure BIOS. Details are in [IPMI]. To enter the BIOS Setup utility press the <Del> key at bootup BEFORE logging into the IPMI Web GUI. Follow the directions in [IPMI] to configure BIOS. **Note that the default BIOS password is ADMIN or changeme, depending on hardware; this must be changed on first use.**
- Configure IPMI. [Install] Instructs the installer to log into the IPMI Web GUI and change the manufacture default IPMI password. Details are in [IPMI]. **Note that the default IPMI password is ADMIN or changeme, depending on hardware; this must be changed on first use.**

3. Reboot again. Following the reboot, SPS attempts to receive an IP address.

   At power up, SPS attempts to receive an IP address automatically via DHCP. If it fails to obtain an automatic IP address, SPS starts listening for HTTPS connections on the `192.168.1.1` IP address. For details on the network interfaces and configuring an initial workstation, refer to [Admin] **The concepts of One Identity Safeguard for Privileged Sessions (SPS) > Network Interfaces.**

4. Log in to the local console using the default credentials root/default. **The password for the console root admin must be changed on first use.** Any additional configuration on the console as part of the initial setup is not relevant with respect to the product's security functionality and can be configured as needed (e.g. if the IP address needs to be configured manually because DHCP or 192.168.1.1 cannot be used during the setup process).

5. Complete the Welcome Wizard.

   Connect to the SPS web interface from a client machine and complete the Welcome Wizard as described in [Admin] **The Welcome Wizard and the first login**. The Welcome Wizard will walk an installer through the following tasks.

   - Access the SPS web interface. For first time setup, there are no credentials. **The password for the default admin must be set on first use**.
   - Upload the SPS license.
   - Configure the initial system's addresses and names: the SPS physical interface; the default GW; the hostname; the domain name; the DNS server; the syslog server; the SMTP server; the Administrator's email address; and the time zone.
   - Upload or create a certificate and private key for the SPS web interface.
   - Finish configuration via the Welcome Wizard

6. The product is initially deployed with software version 6.0.0. After initial setup, it is necessary to update the product to the latest 6.9 release; refer to the FMT_MOF.1/ManualUpdate section of the document below for information on how to do this.

7. Once initial setup is performed, the additional configuration steps described in the sections below must be followed to ensure the product is deployed into its evaluated configuration.

Security Audit (FAU)

FAU_GEN.1 Audit Generation

One Identity SPS has the ability to generate audit records for security-relevant events. To ensure that sufficiently detailed system logs are generated, the following configuration options should be applied:

- On the Web UI, navigate to Basic Settings > Management and select “Enable” under Verbose system logs.
- To change the log verbosity level, navigate to <protocol name> Control > Global Options and set “Verbosity level” to 7. Note that the values set for this correspond to the following logging behavior:
    - 1: logging disabled—do not apply this setting
    - 4: default setting
    - 6-7: debugging information without logging known sensitive data—used for troubleshooting on an as-needed basis
    - 8-10: extremely detailed debugging information which may also include sensitive data—to be used only in extreme troubleshooting issues. If this is enabled, care must be taken to ensure that sensitive data is disposed of properly (e.g. by temporarily disabling external logging or purging the external log records that are generated during this process)

All security-relevant audit events listed below are generated with the default log verbosity level, with the exception of initiating manual updates, which requires a debug level (6-7) to be set.

The following table identifies sample audit records for the claimed security requirements.

Table 3 Example Audit Records

Requirement	Auditable Events	Example Audit Record

FAU_GEN.1	Start-up and shutdown of the audit functions	`2022-01-27T12:08:23-05:00 oneidentity-sps-boot systemd[1]: Stopping System Logger Daemon...`
		
		`2022-01-27T12:11:39-05:00 oneidentity-sps-boot systemd-nspawn[5813]: [* ] A start job is running for System Logger Daemon (5s / 1min 30s) [K[ OK ] Started System Logger Daemon.`

FAU_GEN.2	None	n/a
FAU_STG_EXT.1	None	n/a
FCS_CKM.1	None	n/a
FCS_CKM.2	None	n/a
FCS_CKM.4	None	n/a
FCS_COP.1/DataEncryption	None	n/a
FCS_COP.1/SigGen	None	n/a
FCS_COP.1/Hash	None	n/a
FCS_COP.1/KeyedHash	None	n/a
FCS_HTTPS_EXT.1	Failure to establish a	`2021-10-05T12:16:11-04:00 oneidentity-sps.leidos.ate nginx: *1259 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared`

	HTTPS Session	cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:14-04:00 oneidentity-sps.leidos.ate nginx: *1260 accept: 172.16.0.161:60556 fd:3 2021-10-05T12:16:14-04:00 oneidentity-sps.leidos.ate nginx: *1260 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1261 accept: 172.16.0.161:60558 fd:3 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1261 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1262 accept: 172.16.0.161:60560 fd:3 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1262 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:21-04:00 oneidentity-sps.leidos.ate nginx: *1263 accept: 172.16.1.50:1110 fd:3
FCS_RBG_EXT.1	None	n/a
FCS_SSHC_EXT.1	Failure to establish an SSH session	2021-09-21T11:24:30-04:00 oneidentity-sps.leidos.ate zorp/scb_ssh[31432]: ssh.error(3): (svc/mCBzJX7ZJqTqsfMbq14HLp/safeguard_default:28/ssh): Unable to find a matching algorithm; type='mac', proxy_algos='hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96', client_algos='hmac-md5', direction='client_to_server', side='client' 2021-09-21T11:24:30-04:00 oneidentity-sps.leidos.ate zorp/scb_ssh[31432]: ssh.error(2): (svc/mCBzJX7ZJqTqsfMbq14HLp/safeguard_default:28/ssh): Error negotiating common algorithms; side='client' 2021-09-21T11:24:30-04:00 oneidentity-sps.leidos.ate zorp/scb_ssh[31432]: ssh.error(3): (svc/mCBzJX7ZJqTqsfMbq14HLp/safeguard_default:28/ssh): Error processing SSH packet; length='755', msg='20', side='client' 2021-09-21T11:24:30-04:00 oneidentity-sps.leidos.ate zorp/scb_ssh[31432]: scb.audit(4): (svc/mCBzJX7ZJqTqsfMbq14HLp/safeguard_default:28/ssh): Closing connection; connection='safeguard_default'
FCS_SSHS_EXT.1	Failure to establish an SSH session	2021-10-05T15:38:06-04:00 oneidentity-sps-boot sshd[18854]: Unable to negotiate with 172.16.0.161 port 54670: no matching cipher found. Their offer: aes128-cbc [preauth] 2021-10-05T15:38:08-04:00 oneidentity-sps-boot sshd[18857]: Unable to negotiate with 172.16.0.161 port 54672: no matching cipher found. Their offer: aes128-cbc [preauth]
FCS_TLSC_EXT.1	Failure to establish a TLS Session	2021-10-05T10:57:17-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: Certificate validation failed; subject='CN=tlss.leidos.ate', issuer='CN=RootCA_SPS', error='certificate has expired', depth='0' 2021-10-05T10:57:17-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: SSL error while writing stream; tls_error='SSL routines:tls_process_server_certificate:certificate

		verify failed', location='/etc/syslog-ng/syslog-ng.conf:458:9' 2021-10-05T10:57:17-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: I/O error occurred while writing; fd='24', error='Broken pipe (32)' 2021-10-05T10:57:17-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: Syslog connection broken; fd='24', server='AF_INET(172.16.0.25:7514)', time_reopen='60'
FCS_TLSC_EXT.2	None	n/a
FCS_TLSS_EXT.1	Failure to establish a TLS Session	2021-10-05T12:16:11-04:00 oneidentity-sps.leidos.ate nginx: *1259 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:14-04:00 oneidentity-sps.leidos.ate nginx: *1260 accept: 172.16.0.161:60556 fd:3 2021-10-05T12:16:14-04:00 oneidentity-sps.leidos.ate nginx: *1260 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1261 accept: 172.16.0.161:60558 fd:3 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1261 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1262 accept: 172.16.0.161:60560 fd:3 2021-10-05T12:16:15-04:00 oneidentity-sps.leidos.ate nginx: *1262 SSL_do_handshake() failed (SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) while SSL handshaking, client: 172.16.0.161, server: 172.16.16.20:4430 2021-10-05T12:16:21-04:00 oneidentity-sps.leidos.ate nginx: *1263 accept: 172.16.1.50:1110 fd:3
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	2022-02-01T15:55:10+01:00 cctest.bajnok.balabit authdaemon[1996]: Starting; action='Authentication', client_address='192.168.59.1', type='password' 2022-02-01T15:55:10+01:00 cctest.bajnok.balabit scb/authcli[23694]: ALERT (nnxauthd@localhost) Authentication denied, too many attempts, remote_addr is locked out; username='admin', remote_address='192.168.59.1', lockout='60' 2022-02-01T15:55:10+01:00 cctest.bajnok.balabit authdaemon[1996]: Finishing; action='Authentication', client_address='192.168.59.1', type='password' 2022-02-01T15:55:10+01:00 cctest.bajnok.balabit authdaemon[1996]: Authentication failed; client_address='192.168.59.1', type='password', username='admin' 2022-02-01T15:55:10+01:00 cctest.bajnok.balabit restserver[864]: User authentication failed; realm='Balabit', username='admin'
FIA_PMG_EXT.1	None	n/a
FIA_UIA_EXT.1	All use of identification and authenticatio n mechanism.	2022-01-12T10:22:18-05:00 oneidentity-sps.leidos.ate authdaemon[1800]: Starting; action='Authentication', client_address='172.16.1.50', type='password' 2022-01-12T10:22:18-05:00 oneidentity-sps.leidos.ate authdaemon[1800]: Finishing; action='Authentication', client_address='172.16.1.50', type='password'

		2022-01-12T10:22:18-05:00 oneidentity-sps.leidos.ate authdaemon[1800]: Authentication succeeded; client_address='172.16.1.50', type='password', username='admin' 2021-10-05T15:45:57-04:00 oneidentity-sps.leidos.ate authdaemon[1911]: Authentication failed; client_address='172.16.1.50', type='password', username='admin' 2021-10-05T15:45:57-04:00 oneidentity-sps.leidos.ate restserver[1066]: User authentication failed; realm='Balabit', username='admin'
FIA_UAU_EXT.2	All use of identification and authenticatio n mechanism.	2022-01-12T10:22:18-05:00 oneidentity-sps.leidos.ate authdaemon[1800]: Starting; action='Authentication', client_address='172.16.1.50', type='password' 2022-01-12T10:22:18-05:00 oneidentity-sps.leidos.ate authdaemon[1800]: Finishing; action='Authentication', client_address='172.16.1.50', type='password' 2022-01-12T10:22:18-05:00 oneidentity-sps.leidos.ate authdaemon[1800]: Authentication succeeded; client_address='172.16.1.50', type='password', username='admin' 2021-10-05T15:45:57-04:00 oneidentity-sps.leidos.ate authdaemon[1911]: Authentication failed; client_address='172.16.1.50', type='password', username='admin'
FIA_UAU.7	None.	n/a
FIA_X509_EXT.1 /Rev	Unsuccessful attempt to validate a certificate	2021-10-05T00:00:53-04:00 oneidentity-sps.leidos.ate systemd[1]: Started Refresh CRL files. 2021-10-05T00:00:53-04:00 oneidentity-sps.leidos.ate crl-refresh[20265]: CRL refresh error; crl='http://172.16.0.161/sps_crl/IntermediateCRL.pem', error="Unable to download remote CRL. As a result, connections where the Trust Store with name 'SPS_CRL_Test' was configured may be rejected." 2021-10-05T00:00:53-04:00 oneidentity-sps.leidos.ate crl-refresh[20265]: Refresh CRL files: some CRLs failed to update
	Any addition, replacement or removal of trust anchors in the TOE's trust store	2021-10-05T14:17:36-04:00 oneidentity-sps.leidos.ate restserver[1066]: [Changelog-Vf4W8zbCng] Configuration is changed by admin@172.16.1.50 on backend RestConfiguration 2021-10-05T14:17:36-04:00 oneidentity-sps.leidos.ate restserver[1066]: [Changelog-Vf4W8zbCng] Element removed: trust_stores/855257bd-75f9-4bf5-82b9-f44f9d237bd4[name='Test213123'] 2021-10-05T14:17:36-04:00 oneidentity-sps.leidos.ate lockingconfigstatedaemon[247]: Starting; action='Loading configuration' 2021-10-05T14:17:28-04:00 oneidentity-sps.leidos.ate nginx: *1317 172.16.1.50 - - "DELETE /api/configuration/trust_stores/855257bd-75f9-4bf5-82b9-f44f9d237bd4 HTTP/1.1" 200 500 "https://172.16.16.20/portal/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0" 2021-10-05T14:17:28-04:00 oneidentity-sps.leidos.ate restserver[1066]: Content of the "Host" header: 172.16.16.20
FIA_X509_EXT.2	None	n/a
FIA_X509_EXT.3	None	n/a

FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	2022-01-27T15:54:20-05:00 oneidentity-sps.leidos.ate scb/web: DEBUG (admin@172.16.1.50) Preparing command; cmd=''/opt/scb/bin/firmwarectl' 'install' '/opt/scb/tmp/xcb-upload-HkmS7X''
FMT_MTD.1/CoreData	None	n/a
FMT_MTD.1/CryptoKeys	None	n/a
FMT_SMF.1	All management activities of TSF data.	Refer to Table 4 below.
FMT_SMR.2	None	n/a
FPT_APW_EXT.1	None	n/a
FPT_SKP_EXT.1	None	n/a
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	2021-10-05T12:18:48-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Setting Date & Time; timestamp='1633447125' 2021-10-05T12:18:48-04:00 oneidentity-sps-boot scb/daemon[2745]: INFO (root@localhost) Setting time; timestamp='1633447125' 2021-10-05T11:18:45-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Configuration is changed by admin@172.16.1.50 on backend BasicDatetime 2021-10-05T11:18:45-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at Manual time settings changed from 2021-10-05 12:18:48 to 2021-10-05 11:18:45 2021-10-05T11:18:45-04:00 oneidentity-sps-boot xcbdaemon[2745]: Tue Oct 5 15:18:45 UTC 2021
FPT_TST_EXT.1	A self-test failed.	The TOE will not be in a state where it is capable of writing to the system log if a self-test fails.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	The successful update process creates an entire update log file. The file is below.  upgrade.1639770645.log The following record is from a failed update. 2022-01-27T15:54:20-05:00 oneidentity-sps.leidos.ate scb/web: DEBUG (admin@172.16.1.50) Running command finished; exit_code='1', as_root='true', background='false', cmd=''/opt/scb/bin/firmwarectl' 'install' '/opt/scb/tmp/xcb-upload-HkmS7X'' 2022-01-27T15:54:20-05:00 oneidentity-sps.leidos.ate scb/web: ERROR (admin@172.16.1.50) Cannot install firmware; This version (6.9.4.rc2) is already installed.
FTA_SSL_EXT.1	The termination of a local	2022-01-27T14:22:50-05:00 oneidentity-sps.leidos.ate sudo: pam_unix(sudo:session): session closed for user roottimeout

	session by the session locking mechanism.	
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	2021-10-05T10:41:31-04:00 oneidentity-sps.leidos.ate authdaemon[1911]: User session has ended; address='172.16.1.50', backend='local', reason='expiry', username='admin' 2021-10-05T10:41:31-04:00 oneidentity-sps.leidos.ate scb/web: ERROR (admin@172.16.1.50) Session timeout error; Session timed out or has been terminated, please log in.
FTA_SSL.4	The termination of an interactive session.	2021-10-05T10:41:31-04:00 oneidentity-sps.leidos.ate scb/web: ERROR (admin@172.16.1.50) Session timeout error; Session timed out or has been terminated, please log in.
FTA_TAB.1	None	n/a
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	2021-10-05T10:49:09-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: Syslog connection established; fd='18', server='AF_INET(172.16.0.25:7514)', local='AF_INET(0.0.0.0:0)' 2021-09-29T08:03:02-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: Syslog connection failed; fd='20', server='AF_INET(172.16.0.25:7514)', error='Connection refused (111)', time_reopen='60'
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions	2021-10-05T10:49:09-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: Syslog connection established; fd='18', server='AF_INET(172.16.0.25:7514)', local='AF_INET(0.0.0.0:0)' 2021-09-29T08:03:02-04:00 oneidentity-sps.leidos.ate syslog-ng[113]: Syslog connection failed; fd='20', server='AF_INET(172.16.0.25:7514)', error='Connection refused (111)', time_reopen='60'

The following table identifies sample audit records for administrative actions that are considered to be security-relevant with respect to the TOE claims:

Table 4 Management Commands Audit Records

Admin Action	Example Audit Record
Ability to configure the access banner	2021-10-05T15:30:27-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/management/auth_banner

Admin Action	Example Audit Record
	changed from Unauthorized access to this system is forbidden and will be 2021-10-05T15:30:27-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) prosecuted by law. By accessing this system, you agree that your actions 2021-10-05T15:30:27-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) may be monitored if unauthorized usage is suspected. 2021-10-05T15:30:27-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Test123123123 to Unauthorized access to this system is forbidden and will be 2021-10-05T15:30:27-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) prosecuted by law. By accessing this system, you agree that your actions 2021-10-05T15:30:27-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) may be monitored if unauthorized usage is suspected. 2021-10-05T15:30:27-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Test123123123000000
Ability to configure the session inactivity time before session termination or locking	2021-10-05T15:35:10-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Configuration is changed by admin@172.16.1.50 on backend BasicManagement 2021-10-05T15:35:10-04:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/management/session_timeout changed from 10 to 312
Ability to configure the authentication failure parameters for FIA_AFL.1	2022-01-27T20:15:49-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Configuration is changed by admin@172.16.1.50 on backend AuthSettings 2022-01-27T20:15:49-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/aaa/settings/backend/password_check/modified changed from 1643332507 to 1643332546
Ability to configure audit behaviour (e.g. changes to storage locations for audit)	2022-01-27T20:14:21-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Configuration is changed by admin@172.16.1.50 on backend BasicManagement 2022-01-27T20:14:21-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/management/syslog_server_auth/trust_store/idref changed from Pascal1 to AuditTest
Ability to manage the cryptographic keys	Need 2022-01-27T20:28:33-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-lZjAjDevin] Configuration is changed by admin@172.16.1.50 on backend RestConfiguration 2022-01-27T20:28:33-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-lZjAjDevin] Element removed: trust_stores/ee53c445-1a6e-433c-8cd1-a2a33cff675b[name='AuditTest']
Ability to configure the cryptographic functionality	2022-01-27T20:02:56-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-bhKevIaQrs] Configuration is changed by admin@172.16.1.50 on backend RestConfiguration 2022-01-27T20:02:56-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-bhKevIaQrs] Element at management/tls_security_settings/minimum_tls_version changed from "TLSv1_2" to "TLSv1_1"
Ability to manage the TOE's trust store and designate X.509v3 certificates as trust anchors	2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] Configuration is changed by admin@172.16.1.50 on backend RestConfiguration 2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] New element added: trust_stores/ee53c445-1a6e-433c-8cd1-a2a33cff675b[name='AuditTest'] 2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] Element at trust_stores/ee53c445-1a6e-433c-8cd1-a2a33cff675b[name='AuditTest']/trust_store_type changed from "" to "custom" 2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] Element at trust_stores/ee53c445-1a6e-433c-8cd1-

Admin Action	Example Audit Record
	a2a33cff675b[name='AuditTest']/authorities/0 changed from "" to "-----BEGIN CERTIFICATE----- \nMIIDHDCCAgSgAwIBAgIIWI0NxI/WJPwwDQYJKoZIhvcNAQELBQAwFDESMBAGA1UE\nAxMJQXVkaXRUZXN0MB4XDTIyMDExMTIxMTUwMFoXDTMyMDExMTIxMTUwMFowFDES\nMBAGA1UEAxMJQXVkaXRUZXN0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC\nAQEAvInjiTYI5Nj9MgEedrUtT+5MZuwA+ctyjFsRC/xo8S0fohBVw0l/lARXxpWn\nQ7SawqKItya9lVm1B/TqsGHWpj0mmyQV9sEN82NNhJiaJyk0Uojts5kubL7sNwUg\nv8LJ6R/ij0gkaK40X6I/s3cvPX7EGtKrrK/MT7zzN5kfcyrnPNROhGALgCOOUntw\nkTq9Nv4Y3MmMk1Fhhs/rIuycSnKDeVHIXNnshXNbjDE20iD+MVgARHHhGDxzThWS\n1By7QW5H8RBDfKhlB2LfGvT4XNEpUriPfG4MhceYfpMU1k5X9PHCpZLhluxvh+PV\nd9nh55tHK9YH/tBxmRp49gcvlwIDAQABo3IwcDAPBgNVHRMBAf8EBTADAQH/MB0G\nA1UdDgQWBBS1/All b2RDYBb9/L1rjWSZTyR8wTALBgNVHQ8EBAMCAcYwEQYJYIZI\nAYb4QgEBBAQDAgAHMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2VydGlmaWNhdGUwDQYJ\nKoZIhvcNAQELBQADggEBALlTk5pKl8vYMnJgBgrp1XzaS3ZNXroenoAH4ltmpLr5\niMNLj/VymEa0VapDfn6kVOijt2AW7LIoMmFqLgzL3L8EBu8iQAqNP0B56E1bP+Rn\nB8wHLFuHZSvMPN1Xgvqomz/3w2xpd+Dphpga1fZraxdsQ6BgMaxEeNOTHHYNLAl1\nP4qkW6SWOCZTAJ0b4eP1lBWhZB3rhlyH1hQjZNCI3IntKA6Z+0uZD4CvuwTKRtm/\n81rhuwSGA3QpvoeTixUAPM0KOSEmMi1kf61ebL3DKTU6xz3xMfuKYI4Omj1rN45Q\nmtiHno4LwEHu4RK3dvL9TKHx3Ck2kjevO4wfC018JOg=\n-----END CERTIFICATE-----\n" 2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] Element at trust_stores/ee53c445-1a6e-433c-8cd1-a2a33cff675b[name='AuditTest']/name changed from "" to "AuditTest" 2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] Element at trust_stores/ee53c445-1a6e-433c-8cd1-a2a33cff675b[name='AuditTest']/revocation_check changed from "" to "none"
Ability to import X.509v3 certificates to the TOE's trust store	2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] Element at trust_stores/ee53c445-1a6e-433c-8cd1-a2a33cff675b[name='AuditTest']/trust_store_type changed from "" to "custom" 2022-01-27T20:02:41-05:00 oneidentity-sps.leidos.ate restserver[1173]: [Changelog-Uh9Wo5wRvd] Element at trust_stores/ee53c445-1a6e-433c-8cd1-a2a33cff675b[name='AuditTest']/authorities/0 changed from "" to "-----BEGIN CERTIFICATE----- \nMIIDHDCCAgSgAwIBAgIIWI0NxI/WJPwwDQYJKoZIhvcNAQELBQAwFDESMBAGA1UE\nAxMJQXVkaXRUZXN0MB4XDTIyMDExMTIxMTUwMFoXDTMyMDExMTIxMTUwMFowFDES\nMBAGA1UEAxMJQXVkaXRUZXN0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC\nAQEAvInjiTYI5Nj9MgEedrUtT+5MZuwA+ctyjFsRC/xo8S0fohBVw0l/lARXxpWn\nQ7SawqKItya9lVm1B/TqsGHWpj0mmyQV9sEN82NNhJiaJyk0Uojts5kubL7sNwUg\nv8LJ6R/ij0gkaK40X6I/s3cvPX7EGtKrrK/MT7zzN5kfcyrnPNROhGALgCOOUntw\nkTq9Nv4Y3MmMk1Fhhs/rIuycSnKDeVHIXNnshXNbjDE20iD+MVgARHHhGDxzThWS\n1By7QW5H8RBDfKhlB2LfGvT4XNEpUriPfG4MhceYfpMU1k5X9PHCpZLhluxvh+PV\nd9nh55tHK9YH/tBxmRp49gcvlwIDAQABo3IwcDAPBgNVHRMBAf8EBTADAQH/MB0G\nA1UdDgQWBBS1/All b2RDYBb9/L1rjWSZTyR8wTALBgNVHQ8EBAMCAcYwEQYJYIZI\nAYb4QgEBBAQDAgAHMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2VydGlmaWNhdGUwDQYJ\nKoZIhvcNAQELBQADggEBALlTk5pKl8vYMnJgBgrp1XzaS3ZNXroenoAH4ltmpLr5\niMNLj/VymEa0VapDfn6kVOijt2AW7LIoMmFqLgzL3L8EBu8iQAqNP0B56E1bP+Rn\nB8wHLFuHZSvMPN1Xgvqomz/3w2xpd+Dphpga1fZraxdsQ6BgMaxEeNOTHHYNLAl1\nP4qkW6SWOCZTAJ0b4eP1lBWhZB3rhlyH1hQjZNCI3IntKA6Z+0uZD4CvuwTKRtm/\n81rhuwSGA3QpvoeTixUAPM0KOSEmMi1kf61ebL3DKTU6xz3xMfuKYI4Omj1rN45Q\nmtiHno4LwEHu4RK3dvL9TKHx3Ck2kjevO4wfC018JOg=\n-----END CERTIFICATE-----\n"
Ability to create and modify user	2022-01-27T20:35:29-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Configuration is changed by admin@172.16.1.50 on backend AuthLocalusers 2022-01-27T20:35:29-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) New element added: /config/xcb/aaa/usersgroups/users/user 2022-01-27T20:35:29-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/aaa/usersgroups/users/user/name changed from (none) to AuditTestUser 2022-01-27T20:35:29-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at

Admin Action	Example Audit Record
	/config/xcb/aaa/usersgroups/users/user/password changed from [hidden] to [hidden] 2022-01-27T20:35:29-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/aaa/usersgroups/users/user/groups changed from (none) to policies-view, policies-write 2022-01-27T20:35:40-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Configuration is changed by admin@172.16.1.50 on backend AuthLocalusers 2022-01-27T20:35:40-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/aaa/usersgroups/users/user[@name = 'AuditTestUser']/groups changed from policies-view, policies-write to policies-view, policies-write, rdp-view
Ability to configure password policy	2022-01-27T20:15:49-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Configuration is changed by admin@172.16.1.50 on backend AuthSettings 2022-01-27T20:15:49-05:00 oneidentity-sps.leidos.ate scb/web: INFO (admin@172.16.1.50) Element at /config/xcb/aaa/settings/backend/password_check/modified changed from 1643332507 to 1643332546

FAU_GEN.2 User Identity Association

No separate configuration is required for this security function. All audit events that are associated with administrative actions will automatically identify the administrator responsible for performing the function.

FAU_STG_EXT.1 Protected audit event storage

Audit data is stored locally on SPS; in the evaluated configuration, it is also necessary to configure this data to be written to an external syslog server over TLS. Enabling a syslog connection over TLS is described below; the TLS configuration parameters (e.g. supported TLS version and cipher suites) for TLS interfaces is discussed more generally in the "FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol" section below.

When configured, data is written to the external syslog in real time. To reduce the risk of the syslog server not receiving log messages from SPS because of a network outage or other problem with the syslog server, SPS buffers up to 10 MB of log messages or seven days' worth of records (whichever comes first) to local storage in case the syslog server is temporarily inaccessible.

Listed below are the steps to set up the external syslog connection using either the Web UI or REST API.

To Configure a Syslog Server from the Web UI

[Admin] Section **System logging, SNMP and e-mail alerts > Configuring system logging** identifies the parameters to configure the remote syslog server. The section describes the **Basic Settings > Management > Syslog** page. The parameters include the following:

- **Network Address** - The IP address or FQDN of the syslog server
- **Port** - The port number for syslog server
- **Protocol** - The network protocols and syslog header type. The evaluated configuration supports both `Legacy-TCP-TLS` and `Syslog-TCP-TLS` options from the Protocol pull-down menu, as well as unencrypted connections. *The `TCP-TLS` suffix must be selected for the evaluated configuration; the TOE provides encrypted communication with the syslog server*

instead of sending plain text over TCP. The `legacy-` prefix corresponds to the legacy BSD-syslog protocol described in RFC 3164, while the `syslog-` prefix corresponds to the new IETF-syslog protocol described in RFC 5424. The prefix that is selected will depend on what your specific syslog server supports; either format is acceptable as long as TLS is used.

- **Check server certificate** – if selected, SPS will validate the X.509 certificate received from the syslog server. *This parameter is required to be selected in the evaluated configuration.* The administrator is required to identify the trust store name in the pull-down menu of the **Trust Store** parameter. The certificate for the Trust Anchor for the syslog server certificate chain must be loaded in the specified Trust Store. The certificate for syslog server itself must be provided in the TLS session by the syslog server. Certificates for any intermediate Certificate Authorities may be loaded in the Trust Store or supplied by the syslog server. For more information refer to [Admin] section **Managing the certificates used on One Identity Safeguard for Privileged Sessions (SPS) > Uploading external certificates to One Identity Safeguard for Privileged Sessions (SPS).**
- **Authenticate as client** – if selected, SPS will supply an X.509 certificate to the syslog server if the syslog server requests it (mutual authentication). *Mutual authentication is **optional** in the evaluated configuration.* If mutual authentication is used, the Administrator is required to specify the X.509 certificate to send to the syslog server along with the associated private key. This may be an existing certificate (i.e. used for other purposes as well) or a certificate for just this usage. In the latter case, the administrator is required to generate and sign a certificate and store the certificate and associated private key in the Trust Store as described in section FIA_X509_EXT.3 below. Note that if this parameter is not selected and a syslog server requires mutual authentication, the TLS connection to it will fail to be established.

To Configure a Syslog Server from the REST API

[REST] section **Logs, monitoring and alerts > Syslog server settings** identifies the parameters to configure each remote syslog server using the REST API.

An Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to configure a syslog server.

Managing Disk Space

The system will not function when the disk is full, which by definition also means that new audit records cannot be generated when this occurs. The guidance below can be followed to mitigate the risks of disk space exhaustion.

To Configure Disk Fill-up Prevention Parameters from the Web UI

SPS continuously monitors the health of the SPS hardware and its environment. This includes the amount of disk space used. The TOE enables an administrator to specify when to stop SSH clients when a percentage of disk space is reached and enables an administrator to specify a cleanup policy to be performed when the disk space reaches the percentage. Cleanup removes (deletes) old files.

The following parameters apply to prevention of disk space exhaustion. As noted earlier in this section, syslog data is automatically retained for up to 10 MB or seven days; these parameters apply to recordings of privileged session activity, which is outside the scope of the claimed security requirements.

- **Disconnect clients when disks are.** This parameter enables an Administrator to specify that when a percentage of the disk is used above the configured limit, SPS will disconnect all clients. The default value is 80.
  Refer to [Admin] section **Configuring system monitoring on SPS > Preventing disk space fill-up** for guidance about setting parameters to prevent disk space from filling up. An Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation.
- **Automatically start archiving**. This parameter instructs SPS to automatically start all configured archiving/cleanup jobs when disk usage goes over the **Disconnect clients when disks are** limit.
  Refer to [Admin] section **Configuring system monitoring on SPS > Preventing disk space fill-up** for guidance about setting parameters to prevent disk space from filling up. An Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation.
- **Delete data from SPS after**. This cleanup parameter permanently deletes all audit trails and data that is older than the **Delete data from SPS after** parameter without creating a backup copy or an archive. Such data is irrecoverably lost. Use this option with care.
  Refer to [Admin] section **Archiving and Cleanup > Creating a cleanup policy** for guidance. An Administrator needs **read and write/perform** permission to the **Policies** object in order to perform this operation.

To Configure Disk Fill-up Prevention Parameters from the REST API

Refer to [REST] **Logs, monitoring and alerts > Disk fill-up prevention** using the REST API.

Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation and FCS_CKM.2 Cryptographic Key Establishment

SPS implements several key generation and key establishment algorithms. Generally, these functions are not invoked directly by an administrator. Specifically, keys are generated/established in the following circumstances:

- Elliptic curve keys are generated for TLS when a TLS_ECHDE cipher suite is negotiated. Reference the “FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol” section below for information on how to configure the supported TLS cipher suites. This operation does key establishment as well.
- Elliptic curve keys are also generated when a certificate signing request (CSR) is generated. Specifically, there is no option for any other key type for this function, so the act of generating a CSR implicitly generates the key pair as well. Reference the “FIA_X509_EXT.3 X.509 Certificate Requests” section below for information how to generate a CSR.
- Finite field keys are generated for TLS when a TLS_DHE cipher suite is negotiated. Reference the “FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol” section below for information on how to configure the supported TLS cipher suites. This operation does key establishment as well.
- Finite field keys are also generated for SSH as part of the Diffie-Hellman key exchange process. Reference the “FCS_SSHC_EXT.1 SSH Client Protocol and FCS_SSHS_EXT.1 SSH Server Protocol” section below for how to configure the supported SSH key exchange algorithms.

FCS_CKM.4 Cryptographic Key Destruction

SPS provides mechanisms to erase persistently-stored secret keys, as described below.

Certificate signing requests, which include key data, can be deleted by invoking the REST API method HTTP DELETE /api/pki/certificate/requests/<ID-of-the-CSR>.

The product's own TLS server certificate is destroyed by replacement with another certifcate; this is done by using a PUT request to the REST API as described below in FIA_X509_EXT.3.

Trusted CA certificates (for syslog and LDAP connections) are imported when a trust store is configured; reference [Admin] section **Verifying certificates with Certificate Authorities using trust stores**. Specifically, when a trust store is configured, there are buttons for adding/removing certificates that can be used.

The product's own TLS client certificate(s) used for outbound TLS connections (when mutual authentication is enabled) are destroyed by loading a new client certificate or by deselecting the option to authenticate using a client certificate when configuring the connection. Reference [Admin] section **Configuring system logging** and **Managing One Identity Safeguard for Privileged Sessions (SPS) users from an LDAP database** for configuring this behavior for syslog and LDAP, respectively.

SSH server host keys are shown in the SSH Control > Connections page on the Web UI. Under "client side host key settings" the keys for the SSH connection will be listed; the trash can button next to the key string will destroy it or the pencil icon can be used to overwrite it with a new key. More information about SSH host keys can be found in the in the **Setting the SSH host keys offered to the client** section of [Admin].

SSH client keys are loaded into the product when configuring credential stores. This is documented in [Admin] under **Configuring password-protected Credential Stores**.

SSH client keys are loaded into the product when configuring credential stores. This is documented in [Admin] under **Configuring password-protected Credential Stores**. When a client key is loaded into the credential store, it will be listed in the store's contents; the trash can icon is used to delete a key.

The SSH key encryption key (KEK) is used to protect SSH client keys in a password-protected credential store. This key is in turn encrypted with a key that is derived from the master password that is set for the credential store. If the master password is changed or removed, the corresponding key is automatically destroyed. Configuration of password-protected credential stores is discussed in the **Configuring password-protected Credential Stores** section of [Admin].

Ephemeral keys associated with TLS and SSH sessions are automatically destroyed when their session ends. No administrator action for these keys is required.

There are no situations in which key destruction is delayed or the manner of key destruction can be specified; destruction always occurs at the same time and following the same procedure.

FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

The AES encryption algorithms used by the product are a direct consequence of the SSH and TLS configuration settings.

In the evaluated configuration, TLS will be configured to support 128-bit and 256-bit keys in both CBC and GCM mode. Guidance on how to configure this can be found in the "FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol" section below.

In the evaluated configuration, SSH will be configured to support 128-bit and 256-bit keys in CTR mode. Guidance on how to configure this can be found in the "FCS_SSHC_EXT.1 SSH Client Protocol and FCS_SSHS_EXT.1 SSH Server Protocol" section below.

FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

The product automatically supports ECDSA signature generation as a direct result of generating a certificate signing request; no separate configuration is performed to support this. Reference the "FIA_X509_EXT.3 X.509 Certificate Requests" section below for information how to generate a CSR.

The product also supports both RSA and ECDSA signature functions for SSH and TLS where the specific algorithm that is used depends on the connection parameters that are negotiated with the peer. Reference the "FCS_SSHC_EXT.1 SSH Client Protocol and FCS_SSHS_EXT.1 SSH Server Protocol" and the "FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol" sections for guidance on the configuration of SSH and TLS, respectively.

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

The hash algorithms used by the product are used for two purposes: trusted communications, for which the supported algorithms are a direct consequence of the SSH and TLS configuration settings, and self-testing, for which SHA-256 is automatically used with no configuration.

In the evaluated configuration, TLS will be configured to support SHA-1, SHA-256, and SHA-384. Guidance on how to configure this can be found in the "FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol" section below.

In the evaluated configuration, SSH will be configured to support SHA-1, SHA-256, and SHA-512. Guidance on how to configure this can be found in the "FCS_SSHC_EXT.1 SSH Client Protocol and FCS_SSHS_EXT.1 SSH Server Protocol" section below.

FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

The keyed hash algorithms used by the product are used for trusted communications, for which the supported algorithms are a direct consequence of the SSH and TLS configuration settings.

In the evaluated configuration, TLS will be configured to support HMAC-SHA-1, SHA-256, and SHA-384. Guidance on how to configure this can be found in the "FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol" section below.

In the evaluated configuration, SSH will be configured to support HMAC-SHA-1, SHA-256, and SHA-512. Guidance on how to configure this can be found in the "FCS_SSHC_EXT.1 SSH Client Protocol and FCS_SSHS_EXT.1 SSH Server Protocol" section below.

FCS_HTTPS_EXT.1 HTTPS Protocol

The product's web interface is automatically configured to support HTTPS as part of completing the initial setup; refer to "Initial Configuration" above for guidance on how to do this.

Following initial setup, it is necessary to configure appropriate restrictions on the TLS versions and cipher suites that the web interface uses. Reference the "FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol" section below for instructions on how to configure the TLS connection settings.

FCS_RBG_EXT.1 Random Bit Generation

No administrator configuration is required for the RNG Functionality. AES-CTR is used by default.

FCS_SSHC_EXT.1 SSH Client Protocol and FCS_SSHS_EXT.1 SSH Server Protocol

The product implements a proxy SSH client and server interface that is used to mediate access to privileged SSH sessions; this functionality is outside the scope of the evaluation, but the actual SSH channels used for this interface are in scope and must be configured using appropriate settings.

Configuration for both client and server connection settings are described in [Admin] under **Creating and editing protocol-level SSH settings**. The SSH parameters are modified from the **SSH Control** menu. The "Algorithm settings" section of this menu has separate columns for client and server settings; to configure these settings, simply fill out the boxes for each setting in each column.

Note that SSH rekeying occurs by default; no administrative configuration of this function is necessary or possible.

An administrator must have **read and write/perform** permissions to the **SSH Control** object in order to make modifications. The default group is `ssh-write`.

Listed below are the algorithm settings, their default values on initial configuration, and the values that are claimed in the evaluated configuration. The full list of supported values for each algorithm is listed in [Admin] under **Supported encryption algorithms**.

- **KEX algorithms:**
  - **Default:** ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512
  - **Evaluated configuration:** diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, diffie-hellman-group16-sha512
- **Cipher algorithms:**
  - **Default:** aes128-ctr, aes192-ctr, aes256-ctr
  - **Evaluated configuration:** aes128-ctr, aes256-ctr
- **MAC algorithms:**
  - **Default:** hmac-sha2-256, hmac-sha2-512
  - **Evaluated configuration:** hmac-sha2-256, hmac-sha2-512
- **Compression algorithms:**
  - **Default:** none
  - **Evaluated configuration:** none
- **Host key algorithms:**
  - **Default:** ecdsa-sha2-nistp256, ssh-ed25519, rsa-sha2-512, rsa-sha2-256, ssh-rsa
  - **Evaluated configuration:** ecdsa-sha2-nistp256, ssh-rsa

FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSS_EXT.1 TLS Server Protocol

The product supports a large variety of TLS cipher suites and multiple TLS versions. In the evaluated configuration, either TLS 1.1 or 1.2 is supported; TLS 1.0 must be disabled. Additionally, only certain cipher suites are supported. Specifically, the set of supported TLS cipher suites must be limited to the following:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Configuring the cipher settings and version requirements that SPS uses for establishing TLS connections are described in [Admin] section **General connection settings > Verifying certificates with Certificate Authorities using trust stores**. The section describes the parameters on the **Basic Settings > Trust Stores** page, under the **Cryptography Settings** section. An Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation. Once configured, these settings will apply to all TLS interfaces regardless of whether the product acts as the client or the server.

The following parameters are required:

- **Cipher strength** – specifies the cipher string OpenSSL will use. Options are `Recommended` and `Custom`. The evaluated configuration requires the Administrator to select `Custom`. Once selected, a window will appear and enable the Administrator to enter the cipher strings. Enter the following string to restrict the set of supported cipher suites to the above:

  RSA-PSK-AES128-CBC-SHA:RSA-PSK-AES128-CBC-SHA256:RSA-PSK-AES256-GCM-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384

- **TLS version requirements** – specifies supported TLS version. Specify TLS version 1.1 for the minimum TLS version and TLS version 1.2 for the maximum TLS version.

Note that as part of establishing TLS connections, the product will automatically validate the reference identifier of any presented certificate based on hostname or DN. This function occurs automatically and is not configurable. Additionally, when the product is acting as a TLS server, it will automatically use strong algorithms for key establishment, either 2048-bit Diffie-Hellman parameters or secp256r1, depending on whether the negotiated cipher suite is using TLS_DHE or TLS_ECDHE key establishment.

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

The product's outbound TLS client interfaces (for audit and authentication server) optionally support mutual authentication using X.509 certificates. For both interfaces, this is configured using the "Authenticate as client" configuration options for the respective interfaces. Specifically, mutual authentication for syslog is configured under Basic Settings > Management > Syslog, and mutual

authentication for authentication server connectivity is configured under Policies > LDAP Servers – Configuring Encryption.

In both cases, it is necessary to specify the TLS client certificate that the product will use along with the private key that corresponds to the certificate.

Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure management

The product provides a configurable method of authentication failure lockout for unsuccessful remote login attempts. The local console is unaffected by this. The [Admin] section **Protecting against brute-force attacks** includes guidance on the configuration of this behavior. Specifically, in order to enable authentication failure lockout, the "Protect against brute-force attacks" setting must be enabled, though this is enabled by default. When enabled, there are two settings that affect the behavior of this function:

- The **Attempt limit** configures the number of consecutive failed sign-in attempts within the Lockout Window required to lock a user account. The range is 1 to 50 failed sign-in attempts. The default is `20` consecutive failures.
- The **Lockout period** sets the number of minutes a locked account remains locked. The range is `1` to `720`. The default is `20` minutes.

The **Protect against brute-force attacks** parameter blocks the username or the IP address where the login attempt originates based on the following:

- If the number of unsuccessful login attempts from the same IP address with any user name exceeds the threshold, the IP address is blocked.
- If the number of unsuccessful login attempts with a user name from different IP addresses exceeds the threshold, the user name is blocked for all IP addresses.

This function is only configurable over the Web UI; it is not configurable using the REST API. With the exception of the item above, an Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation. The default group is `basic-write`.

The **web lockout counter** is a local parameter used to count down the time when the user is allowed to login again. During the blocking, the blocked users receive the "Unable to authenticate" error message displayed, regardless of whether the credentials are valid or invalid. Rejected authentication attempts that are made during the blocking period do not increase the **web lockout counter**. The **web lockout counter** for a username or IP address is reset if:

- The lockout period elapses.
- The server is rebooted.
- The root user clears the list of blocked users/IP addresses on the **Clear list of blocked users/IPs** option from the **Troubleshooting** page of the text-based physical or SSH console. Note that when an account is unlocked in this manner, all locked accounts are cleared simultaneously; it is not done on a per-account basis.

FIA_PMG_EXT.1 Password Management

Password rules define the complexity requirements for user authentication to SPS. Password policies apply only to locally managed users, and have no effect for SPS users using LDAP/AD. However, these rules apply to all locally managed users, which includes both web UI users as well as the console root user. An Administrator can create rules governing the type of password a user can create:

- **Minimal password strength** parameter sets the required password complexity level. The possible values are disabled, good, and strong. Only `strong` is supported for the evaluated configuration.

  A strong setting requires the password be at least 8 characters that include numbers, letters, special characters, and capital letters. Letters A-Z, a-z, numbers 0-9, the space character, as well as the following special characters can be used: !"#$%&'()*+,-./:;<>=?@[]\^-`{}_|.

- **Minimal password length** sets the minimum number of characters for the passwords. The acceptable values are `8-99`.

The password policies are listed in the **User management and access control > Setting password policies for local users** section in [Admin]. This section describes the parameters on the **Users & Access Control > Settings > Authentication Settings** page. An Administrator needs **read and write/perform** permission to the **AAA** object in order to perform this operation. The default group is `AAA`.

FIA_UAU.7 Protected Authentication Feedback

Password data is obfuscated while it is being entered and only generic “Access-denied” messages are provided for invalid usernames and passwords. There are no preparatory steps required to ensure that authentication data is not revealed while entering for the login information.

FIA_UAU_EXT.2 Password-based Authentication Mechanism

SPS supports password-based and certificate-based authentication methods. Refer to [CCECG] SFR FIA_UIA_EXT.1 User Identification and Authentication for details.

FIA_UIA_EXT.1 User Identification and Authentication

SPS requires administrator authentication for all security functions except for the display of the pre-authentication warning banner. Local console authentication is only done with a locally-defined username and password for the root admin account. Authentication for remote users uses either locally-defined username and password, username and password defined in an external LDAP directory, or X.509 certificates.

For remote users, configuring a given authentication method is global for all users, with one exception: the default admin user is always able to use local username and password, regardless of the configured authentication mechanism.

Steps for configuring other authentication mechanisms is described in the **Managing One Identity Safeguard for Privileged Sessions (SPS) users from an LDAP database** section of [Admin].

An Administrator needs **read and write/perform** permission to the **AAA** object in order to perform this operation. The default group is `AAA`.

The basic parameters include configuration of:

- **Authentication method** – Options are `Password provided by database`, `RADIUS`, and `X.509`. X.509 and RADIUS are not included in the evaluated configuration.
  - When `Password provided by database` is selected, the following parameter applies.
- **User database** – This parameter is applicable when **Authentication method** is set to `Password provided by database`. Options for this parameter are `Local` and `LDAP`.
  - Select `Local` for locally managed users (the default). Refer to ***To configure SPS to authenticate users using the local user database*** below for a description of local user database specific **Authentication Settings** page parameters.

- Select `LDAP` to configure SPS to use the LDAP protocol. If `LDAP` is selected, refer to ***To configure SPS to authenticate users using LDAP/AD*** below for a description of LDAP specific **Authentication Settings** page parameters.

To configure SPS to authenticate users using the local user database

To configure a local user database from the Web UI

By default, SPS users are managed locally on SPS. SPS local user database authentication is configured from the **Users & Access Control > Settings > Authentication settings** page. Local user database authentication is enabled if the page's **Authentication method** parameter is set to `Password provided by database` and the **User database** parameter is set to `local`.

Once the Authentication method is configured, an administrator must follow the following steps to define users.

1. Create users.

   For detailed instructions on how to create local users, refer to [Admin] section **Managing One Identity Safeguard for Privileged Sessions (SPS) users locally > Creating local users in One Identity Safeguard for Privileged Sessions (SPS).**

2. Assign users to groups.

   For details about how to add a usergroup, refer to [Admin] section **User management and access control > Managing local user groups.**

3. Assign privileges to groups.

   For information on how to control the privileges of usergroups refer to [Admin] section **User management and access control > Managing user rights and usergroups.**

To enable any REST API user access to SPS, the user must have privileges to the **REST server** object. The SPS default groups does not include the **REST server** object and therefore, must be configured. Note that the built-in **api** usergroup does not have this privilege by default, it is used to access the **SOAP RPC API** object. For details about adding the **REST server** object to the **api** group, refer to [Admin] section **Managing user rights and user groups > Managing group privileges**.

To Configure a local user database from the REST API

To configure SPS to authenticate users using LDAP/AD

To Configure an LDAP/AD Server from the Web UI

Enabling LDAP authentication automatically disables the access of every local user except for `admin`. The `admin` user can login to SPS even if LDAP authentication is used. SPS LDAP authentication is configured from the **Users & Access Control > Settings > Authentication settings** page. LDAP is enabled if the page's **Authentication method** parameter is set to `Password provided by database` and the **User database** parameter is set to `LDAP`. Refer to [Admin] Section **Managing One Identity Safeguard for Privileged Sessions (SPS) users from an LDAP database** for guidance on the **Authentication settings** page parameters if configured for LDAP. The parameters include configuration of:

- **Network Address** - The IP address or FQDN of the LDAP/AD server
- **Port** - The port number for LDAP server. Port 636 is required in order to select TLS communication.

- **Type** – The type of LDAP server. The options are `Active Directory` and `POSIX`. Select `Active Directory`. `POSIX` is not supported in the evaluated configuration.
- **Encryption** – Select the encryption type. The options are `TLS`, `Disabled`, and `STARTTLS`. Select the `TLS` option. `Disabled` and `STARTTLS` options are not included in the evaluated configuration.
- **Check server certificate** – This parameter is displayed if **Encryption** is set to `TLS`. Available options are `No certificate is required` and `Only accept certificates authenticated by the Trust Store`. Only the `Only accept certificates authenticated by the Trust Store` option is allowed for the evaluated configuration; the `No certificate is required` option will take SPS out of the evaluated configuration.

  If selected, SPS will verify the X.509 certificate received from the LDAP server. The administrator is required to identify the trust store name in the pull-down menu of the **Trust Store** parameter. The certificate for the Trust Anchor for the LDAP server certificate chain must be loaded in the specified Trust Store. The certificate for LDAP server itself must be provided in the TLS session by the LDAP server. Certificates for any intermediate Certificate Authorities may be loaded in the Trust Store or supplied by the LDAP server. For more information refer to [Admin] section **Managing the certificates used on One Identity Safeguard for Privileged Sessions (SPS) > Uploading external certificates to One Identity Safeguard for Privileged Sessions (SPS).**
- **Authenticate as client** – This parameter is displayed if Encryption is set to `TLS`. If selected, the LDAP server requires clients to provide mutual authentication using X.509 certificates for communications with the LDAP server. Mutual authentication is optional in the evaluated configuration.

  If selected, SPS will supply an X.509 certificate to the LDAP server if the LDAP server requests it (mutual authentication). Mutual authentication is optional in the evaluated configuration. If mutual authentication is used, the Administrator is required to specify the X.509 certificate to send to the LDAP server along with the associated private key. This may be an existing certificate (i.e. used for other purposes as well) or a certificate for just this usage. In the latter case, the administrator is required to generate and sign a certificate and store the certificate and associated private key in the Trust Store as described in [CCECG] section FIA_X509_EXT.3. Note that if this parameter is not selected and a syslog server requires mutual authentication, the TLS connection to it will fail to be established.

To Configure an LDAP/AD Server from the Web UI

An administrator can configure LDAP and the corresponding parameters using the REST API. Refer to [Admin] section **User management and access control > Authentication and user database setting** for guidance.

The TOE also supports local administration from its Console interface. Only the `root` user with physical access can access this interface.

Authentication to each interface is documented, as follows:

- Console: **Accessing the One Identity Safeguard for Privileged Sessions (SPS) console** in [Admin]

- Web UI: **Logging in to One Identity Safeguard for Privileged Sessions (SPS) and configuring the first connection** in [Admin]
- REST API: **Authenticate to the SPS REST API** in [REST]

FIA_X509_EXT.1/Rev X.509 Certificate Validation

When X.509 certificates are provided to the product, the product will check the validity of the presented certificates. This includes when the product is acting as a TLS client, when users are being authenticated using X.509 certificates, and when a certificate is loaded onto the product for its own use.

In order for a presented certificate to be validated, the function for which the certificate is being used must be associated with a trust store. The [Admin] section **Verifying certificates with Certificate Authorities using trust stores** includes references on how to configure trust stores and how to associate them with syslog connections, LDAP connections, and user authentication. When a certificate is loaded into the product for its own use, the certificate is validated in one of several ways:

- If a server certificate is uploaded through the web UI, the certificate chain is uploaded along with the server certificate.
- If a client certificate is specified for an outbound TLS connection, the certificate is validated against the trust store specified for the connection.
- If uploaded through the REST API, the operation requires the administrator to specify a trust store to use for validation.

All TLS server certificates must have the Server Authentication purpose set in order to be valid. Because SPS does not use X.509 certificates to validate update packages or validate executable code integrity, no certificates are required to have the Code Signing purpose set. Similarly, because there is no situation where the product is enforcing TLS mutual authentication on TLS clients, there is no situation where the Client Authentication purpose must be set. All certificates for CAs (Trust Anchors and intermediate CAs) must include the basicConstraints extension with the CA flag set to TRUE. Because SPS uses CRLs to check certificate revocation status, no certificates are required to have the OCSP Signing purpose set. All of this functionality is present by default and requires no configuration.

CRL is supported for revocation checking. The revocation checking policy can be configured for a given trust store via Basic Settings > Trust Stores. For a given trust store, three options are present for revocation checking:

- **None** does no revocation check
- **Leaf** checks the revocation status of the peer certificate only
- **Full** checks the revocation status of all certificates in the chain

In the evaluated configuration, “Full” must be selected. For more information, refer to [Admin] section **Verifying certificates with Certificate Authorities using trust stores.**

FIA_X509_EXT.2 X.509 Certificate Authentication

The materials in the previous section describe how to upload certificates into the product and how to configure CRLs to ensure certificate validity.

FIA_X509_EXT.3 X.509 Certificate Requests

Certificates for the product’s own use are typically imported into it after being issued by an external CA. However, the product also has the capability to generate its own certificate signing request to request a certificate to be issued to it.

The process for this is as follows:

1. Generate a private key and certificate signing request
2. Obtain the certificate signing request and send it to a CA
3. Upload the signed certificate back to the product
4. Change the relevant configuration setting to refer to the new certificate.

This is done through the REST API, as documented below.

https://<IP-address-of-SPS>/api/pki/certificate

Cookies

Cookie name	Description	Required	Values
session_id	Contains the authentication token of the user	Required	The value of the session ID cookie received from the REST server in the authentication response, for example, a1f71d030e657634730b9e887cb59a5e56162860. For details on authentication, see **Authenticate to the SPS REST API** in [REST]. NOTE: This session ID refers to the connection between the REST client and the SPS REST API. It is not related to the sessions that SPS records (and which also have a session ID, but in a different format).

Operations

Operations with the /api/pki/certificate endpoint include:

Operation	HTTP method	URL	Notes
Generating a new CSR	POST	/api/pki/certificate/requests	
Adding an X.509 certificate chain to a CSR to create an X.509 identifier	PUT	/api/pki/certificate/requests/<ID-of-the-CSR>	
Setting or replacing a certificate chain for a CSR without knowing the CSR identifier	POST	/api/pki/certificate	X.509 identifier that have been referenced in the configuration will not be updated automatically, when you replace a certificate chain for a CSR. If you

			want to use the newly created X.509 identifier, you must set or update the reference to it in the configuration.
Querying existing CSRs	GET	/api/pki/certificate/requests	
Querying a single CSR	GET	/api/pki/certificate/requests/<ID-of-the-CSR>	
Deleting a CSR	DELETE	/api/pki/certificate/requests/<ID-of-the-CSR>	Deleting a CSR does not remove the corresponding X.509 identifier from the configuration, that is, the existing private key and certificate chain pair remains in use until you update the reference. Unreferenced X.509 identifier are removed automatically

Example: Generating a new CSR

curl --cookie cookies https://<IP-address-of-SPS>/api/pki/certificate/requests

```
{
    “subject”: [
        {“name": "countryName", "value": "US"},
        {"name": "stateOrProvinceName", "value": "CA"},
        {"name": "streetAddress", "value": "4 Polaris Way"},
        {"name": "organizationName", "value":"One Identity"},
        {"name": "commonName", "value": "example.oneidentity.com"},
        {"name": "emailAddress", "value": "info@example.com"}
    ],
    “extensions”: [
        {"critical": true, "name": "basicConstraints", "value": "CA:FALSE"},
```

{"critical": true, "name": "keyUsage", "value": "digitalSignature,keyAgreement"},

{"critical": false, "name": "extendedKeyUsage", "value": "clientAuth"},

{"critical": false, "name": "subjectAltName", "value": "IP:123.123.123.123,DNS:example2.oneidentity.com"

]

}

Elements of the request message body include:

Elements	Type	Description	Notes
subject			
subject.name	string	The subject name must be an object identifier (OID), or a name that can be translated to an OID.	Evaluated configuration uses: • commonName • organizationalName • orgnizationalUnitName • countryName
subject.value	string		
extensions	object	The list of extensions.	Can be null
extensions.name	enum	The name of the extension.	
extensions.value	string	The value of the extension.	Possible values are: • basicConstraints • keyUsage • extendedKeyUsage • subjectAltName • subjectInfoAccess
cxtensions.critical	boolean	Indicates whether the extension should be marked as critical in the request.	

Response

The following is a sample response received when a new CSR is created:

For details of the meta object, see **Message format.**

{

“key": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",

"meta": {

"href": "/api/pki/certificate/requests/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",

"parent": "/api/pki/certificate/requests"

}

}

There are two ways to set or update a certificate chain for a CSR:

- Use a PUT request if the CSR identifier is known
- If the CSR identifier is not known, use a POST request. In this case the REST API automatically selects the CSR based on the information in the first certificate in the chain.

Example PUT request process:

1. Generate a new CSR using the /api/pki/certificate/requests operation
2. Send a GET request to https://<IP-address-of-SPS>/api/pki/certificate/requests/<ID-of-the-CSR> endpoint. Obtain the PEM value of the CSR.
3. Send the CSR to the signing CA and receive the signed certificate.
4. Open a transaction with the REST API as documented in the **Open a transaction** section of [REST]
5. Send a PUT request to https://<IP-address-of-SPS>/api/pki/certificate/requests/<ID-of-the-CSR> that includes the X.509 certificate chain received from the CA and the identifier of the trust store that is used to validate it.

Elements of the message body include:

Elements	Type	Description	Notes
certificate_chain	string or list	The certificate chain can be specified as a string of individual certificates separated by a newline, or as a list of strings containing the certificates. The certificates must be specified in PEM format.	
trust_store	string	The identifier of the trust store that is used to validate the certificate chain, or null, if you want to disable validation.	

The result of this is the X.509 identifier referring to the private key + certificate chain pair.

6. Specify the X.509 identifier to use as the web server certificate. For more information, refer to **Internal certificates** in [REST].

The POST request process is the same for the first four steps. For the fifth step, a POST request must be sent to https://<IP-address-of-SPS>/api/pki/certificate/requests.

The signed CSR may also be uploaded directly through the Web UI. The steps to do this are outlined in the **Managing the certificates used on One Identity Safeguard for Privileged Sessions (SPS)**

Security Management (FMT)

FMT_MOF.1/ManualUpdate Management of Functions in TSF

SPS provides the ability to enable an Administrator to upgrade the version of the TOE. The preparatory steps that are required to upgrade the SPS version are performed outside the TOE boundary however, they are outlined below. Refer to section **Managing One Identity Safeguard for Privileged Sessions (SPS) > Upgrading One Identity Safeguard for Privileged Session (SPS) > Upgrade checklist** in [Admin] for complete information about the checklist that must be performed before upgrading the version of the TOE. Information about upgrading the TOE software/firmware is also found in [Upgrade] more generally.

Checklist summary before an SPS upgrade

- **Determine the version of the current running software/firmware**

  There are three ways an Administrator can view the current version of the running SPS.

  - The **About page** that is displayed upon system boot, displays the running SPS version number. Refer to [Admin] section **The structure of the web interface > About page** for additional detail**.**
  - Navigate to **Basic Settings > System > Version details** to view the version of the running SPS.
  - An administrator can check the system log for the version numbers SPS reported on boot.

- **Determine if an upgrade is available**

  The administrator is required to check for updates and hotfixes; there are no automatic updates or notification that an update is available. An Administrator must have a One Identity (Quest) login account in order to download an upgrade or a hotfix. The account includes a username (email address is required) and a password.

  To determine if an upgrade is available, navigate to the One Identity web site and identify whether the latest version is more recent than the version currently running.

- **Create a configuration backup of SPS (optional)**

  If an upgrade is needed, it is recommended that the administrator backup SPS before upgrading the SPS version. This backup includes configuration information, certificates, and keys and can be used to reinstall or duplicate a new SPS install. Refer to [Admin] section **Archive and backup concepts > Configuration export** for more detail of what is include in a backup file.

  The exported file is gzip-compressed archive that can be decompressed with common archive managers. The **Basic Settings > System > Export configuration** page enables an Administrator to select the encryption method. The evaluated configuration supports both the **Encryption with password** and **GPG encryption** options. Refer to [Admin] section **Upgrading One Identity Safeguard for Privileged Sessions (SPS) > Exporting the configuration of One Identity Safeguard for Privileged Session (SPS)** for detailed information about backing up the SPS. An Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation.

- **Download the file**

  On the support portal, navigate to Support > Download Software > One Identity Safeguard for Privileged Sessions and download the latest install ISO file under Application. Verify the integrity of the downloaded file by computing a SHA-1 hash of the ISO that is published on the Downloads page. This can be done on a Unix system using sha256sum and on a Windows system using Get-FileHash.

  Refer to [Upgrade] for guidance on upgrading a single system. The upgrade process will be the same regardless of version.

  Refer to the FPT_TUD_EXT.1 Trusted Update section below for guidance about uploading the files onto SPS.

FMT_MTD.1/CoreData Management of TSF Data

The product's various management functions with respect to its security claims are referenced throughout this document underneath the corresponding security requirements. The FMT_SMF.1 section below

summarizes all of these functions and identifies where in existing product documentation the instructions for configuring this behavior are described.

FMT_MTD.1/CryptoKeys Management of TSF Data

The product includes functionality for managing the cryptographic keys.

Certificate signing requests, which include key data, are generated and modified using the process described above in FIA_X509_EXT.3.

The product's own TLS server certificate (for the Web UI) is imported using a PUT request to the REST API as described above in FIA_X509_EXT.3.

Trusted CA certificates (for validating server certificates for syslog and LDAP connections) are imported when a trust store is configured; reference [Admin] section **Verifying certificates with Certificate Authorities using trust stores**. Specifically, when a trust store is configured, there are buttons for adding/removing certificates that can be used.

If mutual authentication is used for outbound syslog or LDAP connectivity, the client certificate and public key are uploaded when the connection is configured. Reference [Admin] section **Configuring system logging** and **Managing One Identity Safeguard for Privileged Sessions (SPS) users from an LDAP database** for syslog and LDAP, respectively.

Trusted CA certificates (for validating server certificates for syslog and LDAP connections) are imported when a trust store is configured; reference [Admin] section **Verifying certificates with Certificate Authorities using trust stores**. Specifically, when a trust store is configured, there are buttons for adding/removing certificates that can be used.

SSH server host keys are generated automatically by SPS, but the administrator can also specify their own keys instead if desired. This is done as described in the **Setting the SSH host keys offered to the client** section of [Admin]. Note that this section references ED25519 keys but these are not used in the evaluated configuration, based on the SSH connection settings that are allowed as described in the FCS_SSHC_EXT.1 and FCS_SSHS_EXT.1 section above.

SSH client keys are loaded into the product when configuring credential stores. This is documented in [Admin] under **Configuring password-protected Credential Stores**.

The SSH key encryption key (KEK) is used to protect SSH client keys in a password-protected credential store. This key is in turn encrypted with a key that is derived from the master password that is set for the credential store. The key is generated automatically when a master password is set. If the master password is changed or removed, the corresponding key is automatically destroyed. Configuration of password-protected credential stores is discussed in the **Configuring password-protected Credential Stores** section of [Admin].

FMT_SMF.1: Specification of Management Functions

Security-relevant management functions can be performed at the various management interfaces.
Listed below are the management functions claimed by the product as well as the interfaces where they can be performed from.

- **Ability to configure the access banner (Web UI only)**
  When the access banner is configured, it applies to both the UI and the Console interfaces. The access banner is only configurable using the UI. This is described under **Authentication banner** in [Admin].

- **Ability to configure session inactivity time before session termination or locking (Web UI and REST API)**

  SPS will terminate a user session (UI or Console) if the session is idle for a configurable amount of time. This is described under **Web interface timeout** in [Admin] and **Web interface** in [REST].

  Note that this single setting applies to console, web UI, and REST API sessions.

- **Ability to update the TOE (Web UI only)**

  SPS allows an Administrator to upgrade the TOE software/firmware using the Web UI. This process is described under **Upgrading One Identity Safeguard for Privileged Sessions (SPS) (single node)** in [Admin].

- **Ability to configure the authentication failure parameters for FIA_AFL.1 (Web UI only)**

  SPS allows an administrator to configure authentication failure parameters using the Web UI. This process is described under **Protecting against brute-force attacks** in [Admin].

  Note that the REST API has the ability to enable brute-force protection but the specific parameters for this (attempt limit and lockout period) are not configurable from this interface.

- **Ability to configure audit behaviour (e.g. changes to storage locations for audit records) (Web UI and REST API)**

  SPS allows an administrator to configure the audit behavior with respect to the external server to which audit records are sent. This process is described under **Configuring system logging** in [Admin] and **Syslog server settings** in [REST].

- **Ability to manage the cryptographic keys**

  The functions used to manage keys depends on the key being managed and the operation being performed; refer to the FMT_MTD.1/CryptoKeys section above.

- **Ability to configure the cryptographic functionality (Web UI and REST API)**

  There are two places where the cryptographic functionality is configured: TLS connection settings and SSH connection settings.

  The process for configuring TLS settings is described under **Verifying certificates with Certificate Authorities using Trust Stores** in [Admin].

  The process for configuring SSH settings is described under **Creating and editing protocol-level SSH** settings in [Admin] and under **SSH settings policies** in [REST].

- **Ability to set the time which is used for timestamps (Web UI only)**

  SPS allows an administrator to set the system clock. This process is described under **Configuring date and time** in [Admin].

- **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors (Web UI and REST API)**

  SPS allows an administrator to manage trust stores and to import CA certificates into them, which implicitly designates them as trust anchors. This process is described under **Verifying certificates with Certificate Authorities using trust stores** in [Admin] and **Trust Stores** in [REST].

This operation requires **read and write/perform** permissions for the **Basic Settings** object.

- **Ability to import X.509 certificates to the TOE's trust store (Web UI and REST API)**

  Importing X.509 certificates into the product's trust store follows the same process as mentioned in the previous bullet.

  This operation requires **read and write/perform** permissions for the **Basic Settings** object.

  Separately from this, functionality exists to import TLS client and TLS server certificates into the product for its own use. TLS client certificates are uploaded as part of configuring external syslog and LDAP connections that require TLS mutual authentication; reference **Authenticating users to an LDAP server** and **Configuring system logging** in [Admin]

- **Ability to create and modify users (Web UI only)**

  Local users are created on the Web UI following the guidance specified under **Creating local users in One Identity Safeguard for Privileged Sessions (SPS)** in [ADMIN]. Users can be modified (change password and group membership) from this interface as well.

- **Ability to unlock users (Console only)**

  Locked user accounts are unlocked manually on the local console by navigating to Troubleshooting and selecting the Clear list of blocked users/IPs option.

- **Ability to configure password policy (Web UI only)**

  The process for configuring the password policy for locally-defined users is described under **Setting password policies for local users** in [Admin].

FMT_SMR.2 Restrictions on Security Roles

SPS is managed both locally and remotely. To access SPS via the local console, connect to the chassis serial port. To access SPS via the web interface, open a browser from the workstation and navigate to the URL of the SPS device (which is assigned during initial configuration). To access SPS via the REST API, HTTPS transactions are made with specific individual APIs, all of which are located underneath https://<IP-address-of -SPS>/API; the URLs for individual APIs are documented in [REST]. The web UI and REST API are both locally accessible through direct cable connection to the Ethernet management port if the network is unavailable.

The console interface has one default root user (`root`) that has full privileges over the available functions. This user cannot be deleted. The Web UI/REST API has a default admin user that has full privileges over the available functions. These two accounts can collectively be considered the Security Administrator for the SPS device.

The specification of additional users is not required by the evaluated configuration; it is mentioned here in case specifying additional users with separation of privileges is desired.

SPS also supports additional local users which are role-based users. SPS uses the term group verses roles. SPS provides a set of user groups by default, but custom user groups can be defined as well. Every group has a set of privileges:

- which pages of the SPS web interface (object) a user of that group can access and

- whether that user can only view (read) or also modify (read & write/perform) those pages or perform certain actions.

A user can be assigned multiple groups.

The SPS groups apply to both local users and LDAP users. Local users can be defined in SPS and assigned to groups. Alternatively, LDAP users can be defined and assigned an LDAP group(s) on an LDAP system. Regardless of which system manages the username and passwords, the SPS uses the group associated with the name to determine if the user has the appropriate permission to perform the action on the specific object.

Local users and groups are managed from the **Users & Access Control** page (also referred to as AAA object). Therefore, Administrators must have **read and write/perform** permissions to the **AAA** object in order to make any modifications. Members of the `auth-write` group (a default group), or any other group with write privileges to the `AAA` menu are essentially equivalent to system administrators of SPS, because they can give themselves any privilege.

The following default groups are defined.

Table 5 Default Groups

Group	Object (parent page)	Type (Permission)
basic-view	Basic Settings	read
basic-write	Basic Settings	read and write/perform
auth-view	AAA	read
auth-write	AAA	read and write/perform
Search	Search	read
changelog	AAA/Accounting	read
policies-view	Policies	read
policies-write	Policies	read and write/perform
ssh-view	SSH Control	read
ssh-write	SSH Control	read and write/perform
rdp-view	RDP Control	read
rdp-write	RDP Control	read and write/perform
telnet-view	Telnet Control	read
telnet-write	Telnet Control	read and write/perform
vnc-view	VCN Control	read
vnc-write	VCN Control	read and write/perform
indexing	Search/Search Indexer/Audit Player communication	read and write/perform
ica-view	ICA Control	read

ica-write	ICA Control	read and write/perform
api	Access RPC API privilege	read and write/perform
http-view	HTTP Control	read
http-write	HTTP Control	read and write/perform
indexer-view	Indexer	read
indexer-write	Indexer	read and write/perform

Protection of the TSF (FPT)

FPT_APW_EXT.1 Protection of Administrator Passwords

Local administrative passwords are stored hashed using SHA-512 and salted using 12 bytes of salt (5,000 rounds). This is performed automatically and requires no guidance.

FPT_SKP_EXT.1 Protection of TSF Data (for Reading of all Pre-shared, Symmetric and Private keys)

SPS does not have any native interface to display plaintext key data to an administrator. When backing up the system configuration, the backup bundle may contain sensitive data, so it is necessary to select an option to protect the bundle when the export operation is performed. The **Basic Settings > System > Export configuration** page enables an Administrator to select the encryption method. The evaluated configuration supports both the `Encryption with password` and `GPG encryption` options. Refer to [Admin] section **Archive and backup concepts > Configuration export** and **Exporting the configuration of One Identity Safeguard for Privileged Session (SPS)** for more information. An Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation.

FPT_STM_EXT.1 Reliable Time Stamps

SPS includes a function for the administrator to manually configure the system time. NTP was not tested and is therefore outside the scope of the evaluated configuration.

To configure the date and time, an administrator will use the **Basic Settings > Date & Time** page. Refer to **Configuring date and time** in [Admin] for information on how to perform this function.

The Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation.

FPT_TST_EXT.1 TSF Testing

SPS performs two self-tests; a software/firmware integrity self-test, performed at power on, and a pseudorandom number generator, performed continuously while operational.

If the software/firmware integrity test fails, the failed self-test will be noted on the **About** page of the Web UI. This page will note the boot firmware as “Corrupted” (if the integrity check fails) or “Tainted” (if a firmware file was locally modified). If the PRNG test fails, all production-related services will terminate and the SPS will not be in an operational state.

A failed self-test can also trigger an alert via either SMTP or SNMP. Configuration of SMTP can be found in the **Configuring e-mail alerts** section of [Admin]. Configuration of SNMP traps can be found in the **System related traps** section of [Admin]; the specific trap related to these self-test failures are xcbFirmwareError for the integrity test and xcbRandomGeneratorError for the PRNG test.

In all cases, the administrator action taken in the event of a failed self-test is to contact Support.

FPT_TUD_EXT.1 Trusted Update

SPS provides Administrators with a manual trusted update mechanism used to initiate updates to the product software/firmware. The process for acquiring and verifying updates is described in the FMT_MOF.1/ManualUpdate section above.

TOE Access (FTA)

FTA_SSL_EXT.1 TSF-Initiated Session Locking and FTA_SSL.3 TSF-Initiated Termination

All local and remote sessions are terminated after an administrator-specified time period of interactivity. Specifically, the **Timeout** parameter is configured in the Web UI. Note that while this is found on the "Web interface timeout" page, the same timeout value applies to the local console as well. The **Timeout** parameter specifies the time period of inactivity. The **Timeout** parameter specifies the time period of inactivity. Valid values are between `5` and `720` minutes (12 hours). The default is `10` minutes. When the timeout period is met, a message is displayed and the user can continue or log out.

If there is no activity, the session is terminated. An Administrator needs **read and write/perform** permission

FTA_SSL.4 User-Initiated Termination

The TOE allows administrator-initiated termination of the administrator's own interactive session. The Web UI provides a logout option; the local console supports the `exit` command; and the REST API has the `delete` operation to end a session. Specifically, reference the **Active sessions** section of [REST] for the specific API call used to terminate a session.

FTA_TAB.1 Default TOE Access Banners

SPS has the ability to display a pre-authentication warning banner for both interactive administrative interfaces (Web UI and local console). The same banner text is used for both interfaces.

It is the responsibility of the Administrator to configure the login notification displayed when a user logs into SPS. This feature is typically used for describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. Refer to [Admin] section **Authentication banner** for guidance on defining the authentication banner. The section describes the **Basic settings > Management > Authentication banner** page. An Administrator needs **read and write/perform** permission to the **Basic Settings** object in order to perform this operation.

Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

The product supports trusted channels for audit sever connectivity, authentication server connectivity, and SSH client and server proxying. The list below references where in this document that information on the configuration of these interfaces can be found.

To configure syslog server using TLS

> Refer to [CCECG] section FAU_STG_EXT.1 Protected audit event storage to identify the administrative steps to identify and configure the properties to configure each syslog server.

To configure LDAP/AD server using TLS

Refer to [CCECG] section FCS_TLSC_EXT.1 TLS Client Protocol to identify the administrative steps to identify and configure the properties to configure each LDAP server. Guidance is provided to configure the secure TLS communications channel.

To configure SSH proxy acting as an SSH client or SSH server

Refer to [CCECG] section FCS_SSHC_EXT.1 SSH Client Protocol to identify administrative steps to identify and configure the properties to configure communication an SSH session proxy acting as the SSH client.

To Configure SSH Proxy acting as an SSH server

Refer to [CCECG] section FCS_SSHS_EXT.1 SSH Server Protocol to identify administrative steps to identify and configure the properties to configure communication an SSH session proxy acting as the SSH Server.

The **Basic Settings > Troubleshooting** menu provides a number of diagnostic commands to resolve networking issues. Refer to [Admin] section **Troubleshooting One Identity Safeguard for Privileged Sessions (SPS) > Network troubleshooting for guidance**.

FTP_TRP.1/Admin Trusted Path

Remote administration to SPS is done via HTTPS. HTTPS is automatically configured after the Welcome Wizard has been completed. Invoking the SPS Welcome Wizard is a required step for initial installation of SPS. Once the Welcome Wizard has been completed, an administrator must further configure the system's TLS settings in order to implement the TLS version and cipher suite restrictions needed to place SPS into its evaluated configuration. Refer to [Admin] section **The Welcome Wizard and the first login** for details about completing the Welcome Wizard. Refer to [CCECG] section FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1 for guidance on configuring TLS for the evaluated configuration.

The remote interfaces can be accessed as follows:

Documentation for how to access each of these interface is documented, as follows:

- Web UI: The default URL for the Web UI is https://<ip-address-of-server>. More information can be found in **Logging in to One Identity Safeguard for Privileged Sessions (SPS) and configuring the first connection** in [Admin].
- REST API: Each individual REST API function has its own associated URL. Information on initial authentication can be found in **Authenticate to the SPS REST API** in [REST]; once authenticated, [REST] more generally includes URLs for each supported API under the documentation for each API call.