CACI idt GoSilent Server and Cube v26.01 User Guidance

Document Version: 1.1

Document Date: 23 June 2026

Authored By: CACI idt

2342 Richmond Hwy

Arlington, VA 22202

Revision History

Version	Date	Changes
Version 0.1	July 15, 2025	Initial draft
Version 0.2	August 1, 2025	Added PPK information
Version 0.3	September 15, 2025	Updated PPK info for the Cube and addressed lab OR
Version 0.4	September 29, 2025	Included parameter setting for extra X.509 certificate validation
Version 0.5	October 13, 2025	Added parameter setting for client certificate validation
Version 0.6	March 17, 2026	Added OE and audit information
Version 1.0	May 8, 2026	Addressed evaluator comments
Version 1.1	June 23, 2026	Addressed ECR

Table of Contents

List of Tables

1 Introduction

1.1 Overview

This guide provides supplemental instructions and related information to achieve the Common Criteria evaluated configuration of the GoSilent Server and Cube v26.01 TOE.

1.2 Audience

This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related Security Target.

1.3 Conformance Claims

1.3.1 Common Criteria Conformance

This ST supports the following conformance claims:

- CC version 3.1 revision 5
- CC Part 2 extended
- CC Part 3 conformant

1.3.2 Protection Profile Conformance

This ST and the TOE it describes are exact conformance to the following CC specifications:

- *PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 2.0,* 25 April 2024 (CFG_NDcPP-FW-VPNGW_V2.0)

  This PP-Configuration includes the following components:

  - Base-PP: *collaborative Protection Profile for Network Devices*, Version 3.0e (CPP_ND_V3.0E)
  - PP-Module: *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4e (MOD_CPP_FW_V1.4E)
  - PP-Module: *PP-Module for VPN Gateways*, Version 1.3 (MOD_VPNGW_V1.3)

1.3.3 Evaluated Software and Hardware

The Target of Evaluation (TOE) is the CACI idt GoSilent Server and Cube v26.01:

a) Build: 26.01.1 (GoSilent Server)
b) Build: 26.01.1 (GoSilent Cube)

The TOE includes two physical components:

- GoSilent Server
  - Debian 12 on Red Hat RHEL v9.6 KVM on Intel Xeon Silver 4514Y (Raptor Cove) or
  - Debian 12 on VMware ESXi v8.0 on Intel Xeon Silver 4514Y (Raptor Cove)
- Cube
  - Armbian 25.05 on AllWinner H5/ Cortex-A53 (ARM 8-A)

The Cube is delivered via commercial courier with the software pre-installed. GoSilent Server is a software-only distribution.

1.3.4 Evaluated Functions

The list of evaluated security functions addressed by this evaluation are included in section 1.6 of the Security Target.

1.3.5 Functions Not Included in the TOE Evaluation

The following product functionality is not included in the Common Criteria evaluation:

a) **Cloud instances of GoSilent Server**. GoSilent server is supported on virtual platforms and cloud instances; however, cloud deployments are not addressed by this evaluation.
b) **WiFi connectivity**. The Cube is capable of accepting wireless connections from a client, however no security claims are made with respect to wireless connectivity and is therefore excluded from the evaluation.

1.3.6 Non-TOE Components

The TOE operates with the following components in the environment:

a) Audit Server. The TOE makes use of a syslog server for remote logging.
b) Online Certificate Status Protocol (OCSP) Server/Certificate Revocation List (CRL) Distribution Point (CDP). The TOE communicates with an external OCSP Server and CDP for the purposes of certificate checking.

1.4 Evaluation Assumptions

The following assumptions were made in performing the Common Criteria evaluation as per the PPs and PP-Modules stated in section 1.3.2. The guidance shown in the tabl43e below should be followed to uphold these assumptions in the operational environment.

Table 1: Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	Deploy the TOE in a physically secure environment with controlled access, such as a server room or data centre facility.
A.LIMITED_FUNCTIONALITY	Ensure that the TOE only provides networking functionality as per its core function as outlined in [ST] and is not configured to provide other computing services or general purpose applications which are outside the scope of this document.
A.NO_THRU_TRAFFIC_PROTECTION	Ensure that traffic originating from, or destined to the TOE itself such as administrative traffic and audit data is protected by using secure protocols that leverage encryption and other secure mechanisms of operation.
A.TRUSTED_ADMINISTRATOR	Ensure that administrators are trustworthy and competent by implementing background checks or similar vetting procedures, and providing any relevant or appropriate training.
A.REGULAR_UPDATES	Ensure all relevant updates pertaining to the security and critical functionality of the TOE are applied in a timely and controlled fashion.

ID	Assumption
A.ADMIN_CREDENTIALS_SECURE	Ensure that any passwords or private keys used for the management or administration of the TOE are adequately protected or otherwise secured from theft and unauthorized access on the platform in which they are stored.
A.COMPONENTS_RUNNING	Ensure that each TOE component and its features are operating at nominal and expected levels.
A.RESIDUAL_INFORMATION	Ensure that any storage devices used by the TOE which may contain sensitive residual information are properly purged, destroyed, or otherwise protected from unauthorized access.
A.VS_TRUSTED_ADMINISTRATOR	Ensure that administrators are trustworthy and competent by implementing background checks or similar vetting procedures, and providing any relevant or appropriate training.
A.VS_REGULAR_UPDATES	Ensure all relevant updates pertaining to the security and critical functionality of the TOE are applied in a timely and controlled fashion.
A.VS_ISOLATION	In the context of a virtualized TOE or TOE component, ensure that the VM in which the TOE is running has been appropriately and sufficiently segmented from other VM's and software on the host.
A.VS_CORRECT_CONFIGURATION	Ensure that appropriately trained and experienced personnel have correctly applied or configured settings on the VM in order to support the necessary ND functionality required by the TOE in the operating environment.
A.CONNECTIONS/VPNG	Ensure that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.

1.5 Terminology

The table below defines terms and acronyms used within this document that are not commonly known.

Table 2: Acronyms and Abbreviations

Acronym/Abbreviations	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CRL	Certificate Revocation List
CDP	Certificate Distribution Point
cPP	collaborative Protection Profile
DH	Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral

Acronym/Abbreviations	Definition
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
LAN	Local Area Network
MOD_FW	PP-Module for Stateful Traffic Filter Firewalls
MOD_VPNGW	PP-Module for Virtual Private Network Gateways
NDcPP	collaborative Protection Profile for Network Devices
OCSP	Online Certificate Status Protocol
PP	Protection Profile
PPK	Post-quantum Pre-shared Key
PRF	Pseudorandom Function
PSK	Pre-Shared Key
RFC	Request For Comment
SA	Security Association
ST	Security Target
TLS	Transport Layer Security
TLS/HTTP	HTTP over TLS or HTTPS
TOE	Target of Evaluation
VM	Virtual Machine
VPN	Virtual Private Network
VS	Virtualization Server
WAN	Wide Area Network

2 Secure Acceptance

This section identifies the TOE conformance claims and conformance rationale.

2.1 Obtaining the TOE

The Cube devices are delivered to customers via trusted courier. The following checks should be performed upon receipt:

- Confirm that the correct device has been delivered per the packing slip and original order;
- Inspect all packaging to confirm there are no signs of tampering or damage incurred during transport.

The GSS software can be obtained digitally via URL provided to the customer directly by CACI.

2.2 Installation and Verification

The TOE software comes preinstalled on the shipped hardware. The installed software version can be checked by doing the following:

- **GoSilent Server**
  - Log into the GSS GUI as described in section 3.1 and navigate to the following:

    Maintenance > About
- **GoSilent Cube**
  - Log into the Cube GUI as described in section 3.1 and navigate to the following:

    Help > About This GoSilent

Authorized administrators can perform manual updates to the TOE software by connecting to the component in which they wish to update. Updates are downloaded from a specified URI using HTTPS. All update files are signed with a CACI security key. This signature is checked against the CACI Security Public Key by the TOE upon download and before installation. If the signature check or package upload fails, both the Cube and GSS will not proceed with the installation and instead continue executing the current version. CACI should be contacted for support if subsequent failures occur.

Manual updates to the GSS can be performed by logging into the GSS GUI and navigating to:

Maintenance > Client Firmware

Drag and drop the downloaded image file into the area specified.

Manual updates to the Cube can be performed by logging into the Cube GUI and clicking on the '*Bell*' icon in the top right corner of the GUI and then clicking '*Check for Updates'.*

Prior to the installation of a software update, the Cube will tear down any active tunnels before the update is applied to ensure the integrity of the update process. Once the update process has completed successfully on the Cube, the tunnel is reestablished. On GSS, when an update is successfully installed, GSS will reboot automatically, after which the update will take effect.

Each GoSilent Cube must be registered on the GoSilent Server. Registration involves several steps to be completed by an administrator prior to a Cube establishing a connection to GSS. These steps can be completed by navigating to the *'VPN Clients'* tab in GSS and clicking on the '*Activate*' button next to a listed cube that has been licensed for GSS. The '*Add A Client'* window will appear where the '*Device*

Serial Number' is listed but not configurable. Fill in the '*Client ID'* and '*Client Description'* fields and click '*Add Client*'. Once these steps to prepare the Cube for registration have been completed, a connection attempt from the Cube to GSS can be made.

Note: The first connection attempt from the Cube to GSS will complete the enablement process and may take longer to establish than subsequent connection attempts.

The GoSilent Cube is always the initiator for connections to GSS, therefore should the connection be unintentionally broken during the registration process, the user or administrator should check all network connections for the GSS and the Cube to ensure the integrity of the network and then restart the enablement process described above. Should the enablement process not complete successfully, the administrator can remove the Cube in GSS by navigating to '*VPN Clients'* and clicking the trash can icon ('*Remove'*) next to the Cube experiencing issues, reboot the Cube device, and restarting the Enablement process again.

Cubes may also be suspended and thereby subsequent connections from a cube can be rejected, by also navigating to the *'VPN Clients'* tab in GSS and clicking on the pencil icon beside the Cube to be suspended, toggle the "*Suspend*" button, and click "*Save*".

2.2.1 Factory Reset

GoSilent Cube provides a function to reset itself to the default factory configuration via the web UI. This function is available only to local, direct connections:

a) Connect your computer to the GoSilent Cube via Ethernet;

b) Navigate to "*http://setup.gosilent:8080*" in your browser to reach the Factory Reset page (**WARNING:** Use "http" and not "https");

c) Click the "Reset" button;

WARNING: Do not remove power from the GoSilent Cube or navigate away from GoSilent Cube's Factory Reset page in your browser.

d) Wait for two (2) minutes for the factory reset to complete;

e) Reconnect your computer to the GoSilent Cube via Ethernet;

f) Once complete, navigate to *https://setup.gosilent*

g) Proceed through the Setup Wizard.

3 Configuration Guidance

3.1 Administration Interfaces

Only the following administration interfaces may be used:

a) **GoSilent Server GUI.** Administrative GUI interface for managing all GoSilent configurations on the server and other GoSilent platforms.

- Local access is provided for the configured whitelisted source IP address of an administrator device, and by navigating to the local IP address of GSS through the (virtual) MGMT Ethernet interface using HTTPS via web browser to TCP port 4439.
- Remote access is provided to administrators connecting from Cube clients (for any client that has a valid GSS administrator account) using HTTPS via web browser to the MGMT IP address of the GSS over TCP port 443.

b) **GoSilent Cube GUI.** User GUI interface that provides limited functionality for initial Cube configuration.

- Local access is provided to users by navigating to the local IP address of the cube using HTTPS via web browser over port 4439 or by navigating to the URL https://setup.gosilent.
- Configuration of some Cube functions is done via the GSS GUI. The Cube subsequently downloads these configuration settings from GSS upon connection establishment.

Administrative sessions will be terminated automatically upon reaching the configured inactivity threshold or by the administrator conducting a manual log out action by navigating to the user icon in the top right corner of the GUI and clicking '*Logout*'.

3.2 Setting Time

The GoSilent Server and GoSilent Cube each maintain a system clock used to provide date/time details for use by the TOE.

a) GoSilent Server receives time information from the virtualization platform. Upon startup, the GSS sets its internal clock to that time from ESXi. Subsequently, the GSS internal clock is used and subsequent synchronization with the ESXi clock is not performed. There is a delay in updating the clock until the next GoSilent Server restart. Administrators may also choose to set the time manually on GSS by navigating to the following:

Network > Time and Date

b) GoSilent Cube allows authorized administrators to manually set the time by logging into the Cube GUI and navigating to the following:

Device > Date and Time Settings

Once displayed values have been modified, click *'Set Date and Time'* to apply the changes.

3.3 Firewall Configuration

The TOE performs stateful packet filtering via iptables on all packets sent and received from the External Network, MGMT, and WAN interfaces and applies a uniform policy on all traffic to and from GoSilent Cube users.

To modify the Firewall configurations, navigate to:

'Firewall > Profile and Options'

Ensure the following settings are configured:

- *'Active Firewall Profile'* – Custom Mode must be selected.
- *'Inbound Firewall Option'* – Must be enabled prior to selecting Custom Mode.

Iptables firewall functions are accessible only when "*Custom Mode*" is selected in the '*Firewall > Profile and Options'* GUI. On GSS, select the '*Firewall*' option in the navigation pane and then the '*Advanced Rules'* tab.

Iptables firewall functions are built on the Netfilter framework that is available in the Linux kernel for packet filtering. Netfilter contains **tables**. These tables contain **chains**, and chains contain individual **rules**. If a packet matches any rule, the rule **action** will be applied on that packet.

Firewall rules are processed in the order shown in the GUI (subject to groupings for tables and chains). The GUI presents line numbers for the convenience of the administrator, but they have no significance to iptables.

Administrators can define stateful traffic filtering rules based on a distinct interface in addition to the following network protocol fields:

- ICMPv4 (Type, Code)
- ICMPv6 (Type, Code)
- IPv4 (Source address, Destination address, Transport Layer Protocol)
- IPv6 (Source address, Destination address, Transport Layer Protocol)
- TCP (Source port, Destination port)
- UDP (Source port, Destination port)

Packet filtering rules can be configured with an action to accept (permit/allow), reject (discard/deny), ignore, or to pass the packet on to other rules for more processing.

Netfilter allows the definition of packet filtering rules and processes incoming or outgoing traffic according to the following parameters:

- IPv4 (Request for Comment (RFC) 791)
    - Source Address
    - Destination Address
    - Protocol
- IPv6 (RFC 8200)
    - Source Address
    - Destination Address
    - Next Header (Protocol)
- TCP (RFC 793)
    - Source Port
    - Destination Port

- UDP (RFC 768)
    - Source Port
    - Destination Port

Conformance with the above listed RFCs has been determined through developer testing and as a requirement of this evaluation.

All traffic that correlates to an existing session is permitted, and any traffic not related to a known session is subject to processing by rules that apply flow policies in an administrator-defined order. Rules can be inserted into the ruleset via GUI. Rules are associated to specific interfaces by defining the interface name in the rule. The GUI displays the order of the rules. If no rule matching the traffic exists, the traffic is denied. By default, all traffic from GoSilent Cube users to the External Network, from External Network to Cube users, and between GSS interfaces is denied. A default rule should be applied in the filter table that denies IPv4 and IPv6 source addresses that match the configured IP address on the TOE's interfaces.

The TOE tracks the number of half-open sessions to an administrator-defined threshold. Once this threshold is met, the TOE will discard TCP SYN packets and log the event until the number is below the threshold. By default, half-open TCP connections are discarded after 60 seconds. The following configurable default timeout thresholds (in seconds) are also applied:

a) Generic IP Timeout: 600

b) TCP Connection Timeout: 432000

c) UDP Protocol Timeout: 30

d) UDP Stream Timeout: 180

3.3.1 Iptables Firewall Tables

Netfilter has three unique tables that can contain rules for processing:

a) **Filter table.** The main table for processing network traffic.

b) **NAT table.** Handles all NAT related rules.

c) **Mangle table.** Primarily used for mangling packets.

3.3.2 Table Chains

Each table described in section 3.3.1 can contain chains. These chains are containers for rules in iptables. The Filter table contains the following chains:

a) **FORWARD.** This chain handles packets that have accessed the host, but are destined to another host. Eg. Syslog traffic.

b) **INPUT.** If a packet is coming to the host, it will be processed by this chain.

c) **OUTPUT.** If a packet is going to another host, it will be processed by this chain.

Custom chains can also be created to save rules in. Each chain in the Filter table has a '**policy**', which is the default action taken on packets processed by the chain. The following policies are available:

a) **DROP.** Drops a packet without informing the client.

b) **REJECT.** Drops a packet and informs the sender.

c) **ACCEPT.** Allows the packets to pass the firewall.

The TOE also supports the configuration of rulesets that determine whether traffic is encrypted by using the actions PROTECT, DISCARD, and BYPASS. The TOE enforces a default ruleset that encrypts all traffic between the Cube and GSS. Modification of these default rules, or otherwise configuring rules to bypass encryption between the Cube and GSS is strongly discouraged and outside the scope of the evaluated configuration.

The TOE drops and counts packets that are invalid fragments, and fragmented packets that cannot be re-assembled completely.

By default, the TOE drops packets with the following IP options:

- Loose Source Routing
- Strict Source Routing
- Record Route specified

The TOE logs all actions taken on packets that are processed by the INPUT, OUTPUT, and FORWARD rulesets.

Should a component of the TOE fail, such as the firewall process failing to initialize, the TOE will not enter the state where network traffic can flow. If a failure occurs during operation, the TOE will enter a non-operational state and reboot.

Administrators must configure rules as necessary to ensure the TOE drops and is capable of logging packets in all network traffic that meet the following criteria:

a) Packets where the source address of the network packet is defined as being on a broadcast network (dependent on the TOE's network netmasks, including 255.255.255.255);

b) Packets where the source address of the network packet is defined as being on a multicast network (224.0.0.0/4 for IPv4, ff00::/8 for IPv6);

c) Packets where the source address of the network packet is defined as being a loopback address (127.0.0.1/8 for IPv4, ::1 for IPv6);

d) Packets where the source or destination address of the network packet is defined as being unspecified or an address "reserved for future use" as specified in RFC 5735 for IPv4 (0.0.0.0 or 240.0.0.0/4 for IPv4);

e) Packets where the source or destination address of the network packet is defined as an "unspecified address" or an address "reserved for future definition and use" as specified in RFC 3513 for IPv6 (:: for IPv6, or anything that does not include the prefix '001');

f) Packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;

g) Packets where the source or destination address of the network packet is a link-local address (169.254.0.0/16 for IPv4, fe80::/64 for IPv6);

h) Packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received. (dependent on the specific networks configured by the administrator);

i) Packets where new TCP connections are attempted but exceed the configured limit of half-open TCP connections;

An example configuration of this rule could include the following, however it should be noted that the *--limit-burst* and *--limit 1/s* values can adversely affect performance and reachability if inappropriately configured.

```
-N LOG_THROTTLE_SYN_ACCEPT
-N LOG_THROTTLE_SYN_DROP
-N THROTTLE_SYN
#Throttle SYNs to limit half open TCP connections
-A FORWARD -p tcp --syn -j THROTTLE_SYN
-A THROTTLE_SYN -m limit --limit 1/s --limit-burst 2 -j LOG_THROTTLE_SYN_ACCEPT
# Log accepted SYNs if necessary. (Uncomment next line to enable logging)
#-A LOG_THROTTLE_SYN_ACCEPT -j LOG --log-prefix "[firewall_custom_log] OK "
-A LOG_THROTTLE_SYN_ACCEPT -j ACCEPT
# Log rejected SYNs if necessary
-A LOG_THROTTLE_SYN_DROP -j LOG --log-prefix "[firewall_custom_log] DROP "
-A LOG_THROTTLE_SYN_DROP -j DROP
-A THROTTLE_SYN -j LOG_THROTTLE_SYN_DROP
```

Additional information on the configuration of iptables rulesets can be found here: https://ipset.netfilter.org/iptables.man.html

Additional information on audit logging is described in Section 3.10.

3.3.3 GSS Administrator Access

3.3.3.1 Enable Remote Access

To enable remote access to the GSS GUI from Cube clients, log into the GSS locally and navigate to:

'***Firewall > Profile and Options > Inbound Firewall Option'***

and ensure that the '*Allow GoSilent Clients to connect to the GoSilent Server web interface through the VPN tunnel'* box is checked. Save the configuration.

3.3.3.2 Restrict No-Lockout Access to Whitelisted IP

To restrict no-lockout access to the configured whitelisted source IP address via the (virtual) MGMT Ethernet interface using HTTPS to TCP port 4439, perform the following steps in the GSS GUI:

a) Navigate to '**Firewall > Profile and Options'** tab within the GSS GUI. Then navigate to '**Inbound Firewall Option**' pane and ensure the check box is selected. Click '*Save Inbound Firewall Settings*' button to save the selection.

b) Next, in the '**Active Firewall Profile**' pane, select the '*Custom Mode'* radio button. Click '*Save Active Firewall Profile*' button to save the selection.

c) Navigate to the '**Advanced Rules**' tab.

Note: The necessary rulesets to implement the CC evaluated configuration for local access are already in place by default. This ruleset is labelled in iptables as the 'GSS-MGMT-LOCAL-4439' chain. However, several refinements are required to tailor these rules to the specific network environment.

- Navigate to rule 44 and substitute the IP address of the allowed administrator system.
- Navigate to rule 42 and delete this rule. This rule causes the GSS-MGMT-LOCAL-4430 chain to return before processing the local access configuration rules. Save the configuration.

  Note: Be careful to delete the first instance of this rule in the chain, not the instance at the end of the chain identified as rule 48.

3.3.3.3 Verify Firewall Configuration

Verify the following:

a) The GUI is accessible from the specified whitelist address using TCP port 4439.

b) The GUI is not accessible from other IP addresses via the MGMT interface using port 443 or 4439.

   Note: Any existing connections via TCP port 443 will continue since the rule blocks new connection attempts.

c) Administrator accounts are not subject to account locking when using the local access mechanism.

3.3.3.4 Restrict Access to GSS LAN interface.

Restricting access to the GSS LAN interface may be desired, and can be configured with the following iptables entry:

-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 443 -s <*ip_address*> -j ACCEPT

3.4 Account Lockout

GSS supports account lockout functions resulting from excessive failed login attempts. To modify these functions and the thresholds of GSS, login to the GSS GUI and navigate to the following:

'***System Settings > Admin Console'***

and scroll down to the following settings for administrator defined configuration:

- *'Login attempts before lockout'* (Note: Must be set between 1 and 10)
- *'Lockout interval'* (Note: Must not be 0)
- *'Minimum password length'* (Note: this parameter should be configured to at least 8 characters)

The Cube also supports account lockout functions resulting from excessive failed login attempts. To modify these functions and the thresholds of the Cube, log into the GSS GUI and navigate to the following:

'***System Settings > GoSilent***'

and scroll down to the following settings for administrator defined configuration:

- '*Login attempts before lockout'* (Note: Must be set between 1 and 10)
- *'Lockout interval'* (Note: Must not be 0)

3.4.1 Session Termination

GSS supports automatic termination of inactive local and remote administrative sessions, in addition to manual session termination by an administrator. To modify these functions and the thresholds of GSS, login to the GSS GUI and navigate to the following:

'***System Settings > Admin Console'***

and scroll down to the following settings for administrator defined configuration:

- *'Session inactivity logout interval'* (Note: this parameter must not be '0')

An administrator may terminate their own session by navigating to the user icon in the top right corner of the GUI and selecting '*Logout*'.

The Cube also supports automatic termination of inactive local sessions, in addition to manual session termination. To modify these functions and the thresholds of the Cube, log into the GSS GUI and navigate to the following:

'***System Settings > GoSilent***'

and scroll down to the following settings for administrator defined configuration:

- *'Session inactivity logout interval'* (Note: this parameter must not be '0')
- *'Session inactivity warning interval'* (Note: Must be less than the logout interval if the logout interval is not 0)

A user may terminate their own session by navigating to the user icon in the top right corner of the GUI and selecting '*Logout*'.

3.5 Login Banner

To modify the login banner text for GSS, log into the GSS GUI and navigate to the following:

'***System Settings > Admin Console'***

and scroll down to the '*Enable Login Banner'* setting and ensure the box is checked.

Continue scrolling down to the '*Login Banner Text'* setting and enter the desired login banner message to be displayed.

To modify the login banner text for Cube, log into the GSS GUI and navigate to the following:

'***System Settings > GoSilent***'

and scroll down to the '*Enable Login Banner*' setting and ensure the box is checked.

Continue scrolling down to the '*Login Banner Text*' setting and enter the desired login banner message to be displayed.

3.6 Authentication

To modify the authentication parameters for GSS, log into the GSS GUI and navigate to the following:

'***System Settings > Admin Console'***

and scroll down to the '*Minimum password length'* setting and enter a value. This parameter should be configured to at least 8 characters.

To modify the authentication parameters for Cube, log into the GSS GUI and navigate to the following:

'***System Settings > GoSilent***'

and scroll down to the '*Minimum password length'* setting and enter a value.

This parameter should be configured to at least 8 characters, and up to 40 characters.

The TOE supports the following characters for use in passwords:

a) Upper and lower case letters

b) Numbers

c) Special Characters:

- ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")").

3.7 Firmware Integrity

To modify the integrity checking parameters for GSS, log into the GSS GUI and navigate to the following:

'***System Settings > Admin Console'***

and scroll down to the '*Verify server firmware on boot'* setting and ensure the box is checked.

To modify the integrity checking parameters for Cube, log into the GSS GUI and navigate to the following:

'***System Settings > GoSilent***'

and scroll down to the '*Verify GoSilent firmware on boot*' setting and ensure the box is checked.

On start-up, a firmware integrity test and statistical assessment of the entropy source are executed on both GSS and Cube. If any of these tests fail or otherwise do not complete successfully, the component will not enter an operational state and the network interfaces are not activated. On GSS, a relevant error message is displayed on the local console (accessible via ESXi). On Cube, onboard LEDs indicate the error state and that the system is non-operational.

For the rectification of error states, diagnostic information displayed in relevant error messages on GSS and behaviour of the LEDs on Cube should be referenced. Administrators should contact CACI in the event any component fails the power-up tests.

3.8 VPN

3.8.1 IPsec VPN Configuration

GoSilent Cubes always initiate the connection to establish an IPsec tunnel with GSS.

To modify the VPN parameters of the TOE, log into the GSS GUI as described in section 3.1 and navigate to the following:

'***System Settings > VPN***'

and scroll down to each of the following settings:

- '*IPSec Protocol Mode*' – Set to "IKEv2_Certificates"

- '*IPSec Cipher Suite*' – Default is aes-256gcm16-pfsha512-ecp521 (Top Secret DH21)

  Can configure to:

  aes-256gcm16-pfsha384-ecp384 (Top Secret DH20)
- '*Security Association (SA) Lifetime*' – Between 1 and 24 hours
- '*Child SA Lifetime*' – Between 1 and 8 hours
- '*Enable Strict OCSP Checking*' – Must be enabled

As described further in Section 3.8.3, the TOE employs the user of a network watcher service. The maximum number of retry attempts that will be made by the Network Watchdog service to re-establish the VPN server connection should it fail, or otherwise be unintentionally broken, is configurable (in attempts) to between 0 and 200, with a default configuration of 2 retry attempts. When this threshold is met, the Cube can be rebooted to initiate the connection again. This figure can be configured by navigating to the following:

'System Settings > GoSilent > *Network watcher VPN retries'*

Note: This change will take effect after the user has disconnected and reconnected to the GSS server profile on the Cube Console. The GSS server profile must be set as the default server profile.

Steps for enabling Cubes authorized for connections to GSS can be found in Section 2.2.

3.8.2 Virtual Server Configuration

The GoSilent Cube always initiates the connection to establish a tunnel with GSS. Before the Cube can initiate this connection, a Virtual Server profile containing the GSS server information must be configured on the Cube. This can be done by logging into the Cube by navigating to the following:

Settings > Server Profiles

Click the '*Add*' button next to 'Virtual Server' and enter the details for GSS.

Click '*Add Virtual Server'.* The newly configured server profile for GSS will be shown in the Server Profiles list.

Note: Ensure that all GSS VPN configurations and Cube enablement have been completed as described above.

Click the '*Connect'* button on the GSS server profile. In the '*Are you sure?*' window click '*Yes, I'm Sure'.*

The GSS server profile will show the status '*Connected*'

The '*GoSilent Status'* shown in the top left of the Cube GUI will show '*VPN Connected*'.

3.8.3 Post-quantum Pre-shared Keys Configuration

Post-quantum Pre-shared Keys (PPKs) as defined in RFC 8784 may be used as an enhancement to the standard ECDHE key establishment process. A PPK is an additional secret shared by IPsec endpoints that is stirred into the standard critical security parameters used during key establishment, which provides quantum resistance to the resulting Security Associations (SAs).

PPKs are generated on a third-party system. Since PPK values are secret, they are never displayed after being loaded into GoSilent or directly exchanged between the endpoints during IPsec connection

establishment. Instead, PPKs are referenced via PPK_ID values, which are also generated on the third-party system. A {PPK_ID, PPK} pair is bound together when the values are generated by the third-party system and communicated out of band to authorized administrators. PPKs must be unique, and the PPK_IDs must also be unique. The pair is loaded into the GSS and GSC via the GUI by an authorized administrator. Once loaded, further management of each pair is performed using the PPK_ID only.

PPK_IDs are configured on a per-connection basis. On the GSS, each PPK_ID may be configured for just one VPN Client (e.g. Cube). On the Cube, a single PPK_ID may be configured in more than one profile (e.g. GSS). Since a Cube only has a single active IPsec connection at any time, and any PPK_ID can only be configured for one Cube on each GSS, this scenario ensures that each PPK can only be in use with one IPsec connection at any time.

Usage of PPKs with GoSilent requires several steps. First, the {PPK_ID, PPK} pairs must be loaded onto the GSS and Cubes. Second, the appropriate PPK_ID must be configured on both the GSS and associated Cube. The third step is optional. On the GSS, a parameter may be set to require all IPsec connections to use PPKs. Any connection attempt from a remote endpoint (e.g. Cube) that does not indicate usage of a known PPK_ID that is configured for that endpoint is rejected. If the two endpoints of a connection are configured to use different PPK_IDs, the connection will fail.

If the third step is not performed, then PPKs may be used for IPsec on a per-connection basis. If a PPK_ID is configured for a specific connection in either GSS or Cube, then PPK usage is required for that connection. If a PPK_ID is only configured for one side of the connection, the connection attempt fails.

RFC 8784 defines a per-connection “mandatory_or_not” flag. In GoSilent, this flag is not directly controlled via configuration; it is indirectly set by associated configuration parameters. On the Cube, this flag is set to “mandatory” whenever a PPK is configured for the associated server profile. On this GSS, this flag is set to “mandatory” under any of the following conditions:

- A PPK is configured for the associated client profile.
- The GSS is configured to require PPKs on all client connections (see section 3.8.3.3).

3.8.3.1 Managing PPKs

3.8.3.1.1 GSS

To load a PPK on the GSS, PPK usage must first be enabled. Log into the GUI and navigate to the following:

‘***System Settings***’

Scroll down to the following setting:

- ‘*PPK Secret Size*’ – The default value of “256-bit (Standard)” must always be used.
- ‘*Enable PPK support for IKEv2 clients*’ – Must be enabled.

This step only needs to be performed once, and the GSS must be restarted after enabling the parameter for it to take effect.

Next, log into the GUI and navigate to the following:

‘***Maintenance > Preshared Keys***’

The GUI displays the PPK_IDs that are currently configured in this GSS. Select ‘Add PPK’ to display the Add Preshared Key pop-up window and enter the following information:

- '*PPK_ID* – An alphanumeric value must be entered. If the third-party system generating the PPK_IDs and PPKs supplies a hexadecimal value for the PPK_ID, the hex digits may be entered as the text string.

  (Note: The value entered must be unique on the GSS. If the same PPK_ID value for a PPK is not entered on the GSS and Cube, IPsec connection attempts fail.)

- '*PPK Secret*' – A 256-bit value must be entered as a string of 64 hexadecimal digits.

  (Note: An error message is displayed if the supplied value is not 64 hexadecimal characters.)

- '*Save Preshared Key*' – Select this option to validate the PPK_ID and save the {PPK_ID, PPK} pair in the GSS database. The pop-up window closes and the PPK_ID is shown on the GUI.

  (Note: If validation fails, an error message is displayed, and the values are not saved.)

To delete a {PPK_ID, PPK} pair on the GSS, log into the GUI and navigate to the following:

'***Maintenance > Preshared Keys***'

The GUI displays the PPK_IDs that are currently configured in this GSS. Select the garbage can icon next to the PPK_ID to be deleted. If that PPK_ID is currently associated with any VPN Client (Cube), the PPK_ID is automatically removed from that configuration.

3.8.3.1.2 Cube

Log into the GUI and navigate to the **Device** page. Select Manage next to Preshared Keys.

The GUI displays the PPK_IDs that are currently configured in this Cube. Select 'Add PPK' to display the Add Preshared Key pop-up window and enter the following information:

- '*PPK_ID* – An alphanumeric value must be entered. If the third-party system generating the PPK_IDs and PPKs supplies a hexadecimal value for the PPK_ID, the hex digits may be entered as the text string.

  (Note: The value entered must be unique on the Cube. If the same PPK_ID value for a PPK is not entered on the GSS and Cube, IPsec connection attempts fail.)

- '*PPK Secret*' – A 256-bit value must be entered as a string of 64 hexadecimal digits.

  (Note: An error message is displayed if the supplied value is not 64 hexadecimal characters.)

- '*Save Preshared Key*' – Select this option to validate the PPK_ID and save the {PPK_ID, PPK} pair in the GSS database. The pop-up window closes and the PPK_ID is shown on the GUI.

  (Note: If validation fails, an error message is displayed, and the values are not saved.)

To delete a {PPK_ID, PPK} pair on the Cube, log into the GUI and navigate to the **Device** page. Select Manage next to Preshared Keys.

The GUI displays the PPK_IDs that are currently configured in this Cube. Select the garbage can icon next to the PPK_ID to be deleted. If that PPK_ID is currently associated with any Profile (GSS), the PPK_ID is automatically removed from that configuration.

3.8.3.2 Associating PPK_IDs with IPsec Remote Endpoints

3.8.3.2.1 GSS

To display the PPK_ID associated with an existing Cube, navigate to the following:

'***VPN Clients***'

Select the ellipses icon for the appropriate Cube for More Details and the VPN Client Information pop-up GUI is displayed, which includes any configured PPK_ID.

To associate a PPK_ID with an existing Cube, navigate to the following:

'***VPN Clients***'

Select the pencil icon for the appropriate Cube and the Edit Client pop-up GUI is displayed, and enter the following information:

- '*PPK_ID* (Optional) – Select an unassigned PPK_ID from the drop-down menu.
- '*Save*' – Select this option to save the PPK_ID for the Cube. The pop-up window closes.

To associate a PPK_ID with a new Cube, follow the instructions in section 2.2 to add a client and include the following additional information:

- '*PPK_ID* (Optional) – Select an unassigned PPK_ID from the drop-down menu.

  (Note: The default value is "None Assigned".)

3.8.3.2.2 Cube

To display the PPK_ID associated with an existing Profile, navigate to the following:

'***Server Profiles***'

Select the pencil icon for the appropriate Profile and the Edit Virtual Server pop-up GUI is displayed, which includes any configured PPK_ID.

To associate a PPK_ID with an existing Profile, navigate to the following:

'***Server Profiles***'

Select the pencil icon for the appropriate Profile and the Edit Virtual Server pop-up GUI is displayed, which includes any configured PPK_ID.

- '*PPK_ID* (Optional) – Select a PPK_ID from the drop-down menu.
- '*Save Changes*' – Select this option to save the PPK_ID for the Cube. The pop-up window closes.

To associate a PPK_ID with a new Profile, follow the instructions in section 2.2 to add a Profile and include the following additional information:

- '*PPK_ID* (Optional) – Select a PPK_ID from the drop-down menu.

  (Note: The default value is "None Assigned".)

3.8.3.3 Require all IPsec Connections to Use PPKs

To require all IPsec connections involving a GSS to use PPKs, log into the GSS GUI and navigate to the following:

'***System Settings***'

Scroll down to the following setting:

- '*PPK Mandatory*' – Must be enabled.

This step is optional and should only be performed if PPK_IDs are configured for the VPN Clients (Cubes) that expect to connect to this GSS. The GSS must be restarted after enabling the parameter for it to take effect.

3.9 Network

To modify the Networking parameters of the TOE, log into the GSS GUI and navigate to the following:

'***System Settings > Network***'

and scroll down to each of the following settings:

- '*Enable firewall input logs*' – Must be enabled.

  (Note: Enables logging on the firewall INPUT rules.)
- '*Enable firewall output logs*' – Must be enabled.

  (Note: Enables logging on the firewall OUTPUT rules.)
- '*Enable firewall forward logs*' – Must be enabled.

  (Note: Enables logging on the firewall FORWARD rules.)

The TOE employs the use of a network watcher (Network Watchdog) service that controls the client process that monitors network and VPN connections automatically. The frequency in which to monitor the network and VPN connections is configurable (in seconds) to between 0 (disables the watcher from running) and 300. The default configuration is 2 seconds. This interval can be configured by navigating to the following:

'System Settings > GoSilent > *Network and VPN watcher interval'**.***

Note: This change will take effect after the user has disconnected and reconnected to the GSS server profile on the Cube Console. The GSS server profile must be set as the default server profile.

The maximum number of retry attempts that will be made by the Network Watchdog service to re-establish the internet or WAN connection should it fail, or otherwise be unintentionally broken, is configurable (in attempts) to between 5 and 200, with a default configuration of 5 attempts. When this threshold is met, the Cube can be rebooted to initiate the connection again. This figure can be configured by navigating to the following:

'System Settings > GoSilent > *Network watcher WAN retries'**.***

Note: This change will take effect after the user has disconnected and reconnected to the GSS server profile on the Cube Console. The GSS server profile must be set as the default server profile.

When a device from the LAN network of the Cube tries to communicate through the VPN tunnel, all traffic from the LAN IP address(es) is Port Address Translated (PAT) to the ipsec0 interface address.

Preventing a Cube from communicating through the tunnel can be configured with the following iptables entry:

-A INPUT -i ipsec0 -s <*ip_address*> -j DROP

3.10 Audit Logging

Each TOE component stores its own audit records locally with up to 50MB of audit information across five 10MB files on GSS and up to 1.5MB of audit information across five 300KB files on the Cube. Both components will delete the oldest records first during log rotation.

Each TOE component also transmits a copy of each audit record to an external syslog server in real time via TLS. Syslog server parameters are configured on the GoSilent Server and communicated to all GoSilent Cubes.

Logging of firewall actions taken on packets is configured as described in Section 3.3.

To modify the logging parameters of the TOE, log into the GSS GUI and navigate to the following:

'System Settings > Logging'

and scroll down to each of the following settings:

- '*Enable log shipping*' – Must be enabled.
- '*Log destination host*' – Must be configured.
- '*Log shipping port*' – Must be configured.
- '*Log shipping protocol*' – Must be set to TCP.
- '*Log shipping TLS cipher*' – Default is TLS 1.2: AES128-GCM-SHA256

  Must be configured to one of:

  TLS 1.2: ECDHE-ECDSA-AES256-GCM-SHA384

  TLS 1.3: TLS_AES_256_GCM_SHA384
- '*Reject wildcard TLS server certificates*' – Must be enabled.
- '*Enable CRL checking*' – Must be enabled.

Each Cube will transmit audit log traffic via TLS through the established IPsec tunnel. The IPSec header is then stripped by GSS and traffic is processed by the firewall ruleset which forwards syslog traffic to the syslog server. GSS initiates the connection to the syslog server at startup, and the Cube will initiate a connection to the syslog server once the IPSec tunnel has been successfully established.

If the external syslog server becomes unavailable, or the connection is otherwise unintentionally broken, each TOE component will continue to log locally until the connection is re-established. Attempts to re-establish the TLS channel are automatically made every 5 minutes by each TOE component with no administrator intervention required.

Only authorized administrators may view these audit records (locally or remotely), and no capability to modify or delete the audit record is provided.

3.11 Cryptographic Functions

The TOE performs cryptographic functionality in support of authentication and logging actions. The following key establishment parameters are implemented by the TOE:

a) TLS Client to syslog server – Elliptic-curve (P-384)

b) TLS Server for administrative GUI - Elliptic-curve (P-384, P-521)

c) IKE/IPsec - Elliptic-curve (P-384, P-521)

The TOE performs cryptographic key generation services during IPsec tunnel establishment for IKE peer authentication using ECDSA P-384 and P-521 Elliptic curve keys as specified in FIPS Pub 186-5 “Digital Signature Standard (DSS)” Appendix B.4. These keys are used in the Diffie-Hellman process for IPsec and produce key sizes equivalent to or greater than 192 bits. Additional information on the specification of algorithms used for IPsec connections can be found in Section 3.8.

The TOE performs cryptographic signature generation and verification services using ECDSA P-384 and P-521 in support of IPsec, TLS, X509, and trusted update functions. Additional information on certificate parameters can be found in section 3.12

The TOE only supports TLSv1.2 and TLSv1.3 when acting as a TLS client to provide a trusted channel to the Syslog server. The Cube will always initiate the connection using one of the following ciphersuites:

TLS 1.2: ECDHE_ECDSA_AES256_GCM_SHA384

TLS 1.3: TLS_AES_256_GCM_SHA384

This ciphersuite can be configured as described in sections 3.8 and 3.10.

When the TOE acts as a TLS/HTTPS server to provide the administrative web GUI, TLSv1.2 and TLSv1.3 are supported and use the following ciphersuites:

TLS 1.2: ECDHE_ECDSA_AES256_GCM_SHA384

TLS 1.3: TLS_AES_256_GCM_SHA384

Keyed hash functions are not configurable on their own and are instead included with the overall selection of the desired ciphersuite. For example, ciphersuites using SHA384 will include HMAC-SHA-384.

The RNG functionality provided by the TOE does not require additional configuration.

3.12 Certificate Management

The TOE leverages X509 certificates to provide IPsec connections between GSS and Cube devices, and to verify the identity of the Syslog server.

During the enablement process for a Cube, the X509 certificate for GSS and the specific Cube must be communicated out of band and imported by an authorized administrator for each component. This communication should be done via secure communication channel.

The TOE performs several certificate validity checks on upload, and during TLS and IPsec connection establishment. These checks include a check against its own trust store, the expiration date, revocation status via OCSP (IPSec) and CRL (TLS) and verifies the correct extendedKeyUsage purpose set (Server Authentication). During a certificate upload, the TOE also verifies that the certificate chain terminates

with a trusted CA certificate. When validating a certificate used for IPsec, the reference identifier will be matched against the DN (See below for configuration). Certificates used for TLS connections will fall back to the CN if the SAN is not present.

The TOE supports ECDSA key pair generation using P-384 and P-521 curves which is available through the TOE GUI. When generating certificate signing requests, the option is given to display the CSR information on screen to copy or can be downloaded in PEM format. Keys generated during this process are stored on the TOE in non-volatile memory and are not accessible by any interface. Keys are overwritten when a factory reset is performed.

The TOE supports ECDSA key establishment using P-384 and P-521 curves.

An external CA certificate and key may be loaded onto the system, or a certificate bundle can be loaded into the TOE via the GUI to provide trust for certificate chains and designate trust anchors:

On the Cube, navigate to the following:

'Device > Certificate Management'

Note: During the configuration of the server profile (Virtual Server setup) on the Cube, a drop-down menu is provided to select a certificate to use for the connection.

On GSS, navigate to the following:

'Maintenance > Certificates'

Note: When importing a certificate onto GSS, options for "v2" or "WebDashboard" are provided for the administrator to define the certificate usage.

Certificate signing requests can also be generated through the GUI:

On the Cube, navigate to the following:

'Device > Certificate Management > Manage > Create CSR'

Key size P-384 or P-521 can be selected from the drop-down menu.

On GSS, navigate to the following:

'Maintenance > Certificates > Create CSR'

Key size P-384 or P-521 can be selected from the drop-down menu.

If the TOE fails to contact the OCSP server, the certificate will be rejected and relevant logs will be generated. Administrators should reference these logs when investigating the root cause. If the TOE cannot establish a connection to the CDP, the TOE will accept the certificate.

The TOE must have the following settings configured in the evaluated configuration by navigating to the following:

'System Settings > Logging'

and scroll down to the following settings:

- '*Reject wildcard TLS server certificates*' – Must be enabled.
- '*Enable CRL checking*' – Must be enabled.

'System Settings > VPN'

And scroll down to the following setting:

- '*Enable Strict OCSP Checking*' – Must be enabled

Trusted updates are not verified using X.509 certificates. TLS mutual authentication is not supported.

Administrators may configure both CN and O fields for values that are expected to be present in certificates received from the remote side during IPsec connection setups. The CN value is configurable by default in the '*System Settings > VPN*' menu, however the O value configurability must be enabled using the following steps:

(1) Enable the O value configuration functionality

Log into GSS as an administrator and navigate to ***'System Settings > VPN GUI'.***

The *"Enable Organization for certificate subject name"* check box must be selected.

(2) Restart GSS & Cubes

The GSS must be restarted for a change in this setting to take effect. Each Cube must be restarted three (3) times for a change in this setting to take effect:

(i) Triggers updated settings to be downloaded from GSS

(ii) Cube detects the setting change and reconfigure the network functionality.

(iii) Reconfigured networking functionality to take effect on the Cube.

(3) Configure O value for each applicable Cube on GSS

Log in to the GSS as an administrator and navigate to ***'System Settings > VPN Clients GUI'.*** Add a new cube, or edit an existing Cube entry, and configure the Organization value.

(4) Configure the O value for the GSS on each applicable Cube.

Log in to the Cube as an administrator and select the *'Server Profiles'* page. Add a new profile or edit an existing profile entry and configure the Organization value.

Note: When generating a CSR, the TOE does not include the 'O' value. This must be manually configured per the instructions above, or is the responsibility of the signing CA to insert the 'O' value into the certificate.

The TOE will check the 'O' value if it is present in the certificate.

The GSS must have the following setting configured in the evaluated configuration to enable appropriate X.509 certificate validation by navigating to the following:

'System Settings > Admin Console'

and scroll down to the following setting:

- '*Verify CA chain of client certificate on import*" – Must be enabled.

4 Log Reference

4.1 Format

Each audit record includes the following fields:

a) Date/Timestamp

b) Event Type

c) Subject Identity

d) Event Outcome (Success/Failure)

4.2 Events

The TOE generates the following log events:

Table 3: Audit Events

Associated Requirement	Example Logs
FAU_STG_EXT.1	GoSilent Server: 2026-02-10 14:22:02 INFO Successfully updated default system setting with key (logging.shipping.enabled) with value of (True) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger 2025-10-22T14:15:45-0400 03[CFG] selected proposal: ESP:AES_GCM_16_256/NO_EXT_SEQ 2025-10-22T14:15:45-0400 03[IKE] CHILD_SA 10-1-4-222{67} established with SPIs c73bf491_i 5add4f0f_o and TS 0.0.0.0/0 === 172.16.184.1/32 GoSilent Cube: 2026-01-30 13:34:58 INFO Disabling log shipping... (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/gslogging/log_shipping/shipping.py 119 gosilent.client_framework.app logger
FCO_CPC_EXT.1	**Enabling communications** 2025-10-29T15:44:47-0400 13[IKE] IKE_SA 10-1-4-222[24] established between

Associated Requirement	Example Logs
	10.1.4.149[10.1.4.149]...10.1.4.222[10.1.4.222] 2025-10-22T14:15:45-0400 03[CFG] selected proposal: ESP:AES_GCM_16_256/NO_EXT_SEQ 2025-10-22T14:15:45-0400 03[IKE] CHILD_SA 10-1-4-222{67} established with SPIs c73bf491_i 5add4f0f_o and TS 0.0.0.0/0 === 172.16.184.1/32 GoSilent Cube: 2026-01-30T13:19:10+0000 02[IKE] IKE_SA profile-3-san[9] established between 10.1.4.187[10.1.4.187]...10.1.4.147[10.1.4.147] **Disabling communications** 2025-10-30T13:18:16-0400 09[IKE] no IKE config found for 10.1.4.149...10.1.4.222, sending NO_PROPOSAL_CHOSEN 2026-01-29T12:20:48-0500 06[IKE] deleting IKE_SA 10-1-4-187[8] between 10.1.4.147[10.1.4.147]...10.1.4.187[10.1.4.187] GoSilent Cube: 2026-01-30T14:40:11+0000 16[IKE] sending DELETE for IKE_SA profile-3-san[14] 2026-01-30T14:40:11+0000 16[ENC] generating INFORMATIONAL request 2 [D] 2026-01-30T14:40:11+0000 16[NET] sending packet: from 10.1.4.187[4500] to 10.1.4.147[4500] (65 bytes) 2026-01-30T14:40:11+0000 02[NET] received packet: from 10.1.4.147[4500] to 10.1.4.187[4500] (57 bytes) 2026-01-30T14:40:11+0000 02[ENC] parsed INFORMATIONAL response 2 [ ] 2026-01-30T14:40:11+0000 02[IKE] IKE_SA deleted
FCS_HTTPS_EXT.1	GoSilent Server: 2025-08-07T08:36:11.417347-04:00 10.1.5.12 {"program":"nginx_error","message":"2025/08/07-08:36:23 [info] 5795#5795: *2639 SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking, client: 10.1.4.67, server: 10.1.5.151:443","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","date":"2025-08-07T08:36:23-04:00"} GoSilent Cube: 2025/11/10 09:24:51 [info] 2065#2065: *26 SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking, client: 10.1.3.74, server: 0.0.0.0:443

Associated Requirement	Example Logs
FCS_IPSEC_EXT.1	GoSilent Server: 2025-10-01T12:25:01-0400 06[IKE] no acceptable proposal found 2025-10-01T12:25:01-0400 06[ENC] added payload of type NOTIFY to message 2025-10-01T12:25:01-0400 06[IKE] failed to establish CHILD_SA, keeping IKE_SA GoSilent Cube: 2025-12-19T09:18:59+0000 09[CFG] no issuer certificate found for \"CN=10.1.4.115\" 2025-12-19T09:18:59+0000 09[CFG] issuer is \"CN=ICA1_IKEv2_VM\" 2025-12-19T09:18:59+0000 09[IKE] no trusted ECDSA public key found for '10.1.4.115' 2025-12-19T09:18:59+0000 09[ENC] generating INFORMATIONAL request 2 [N(AUTH_FAILED)]
FCS_TLSC_EXT.1	GoSilent Server: {"timestamp": "2025-09-12 04:00:36", "type": "ERROR", "msg": "Failed to verify the certificate: The certificate does not contain the Server Auth in the Extended Key Usage field", "user": "vpn_server", "userid": "1", "file": "/srv/vpn_edge/./common/certificate/certs.py", "line": 1972, "logger": "gosilent.vpn_server.app logger"} {"timestamp": "2025-09-12 04:00:36", "type": "ERROR", "msg": "Failed to verify a server certificate from 10.1.5.62:6514 (Status code (4114) :: The certificate does not contain the Server Auth in the Extended Key Usage field)", "user": "vpn_server", "userid": "1", "file": "/srv/vpn_edge/./common/gslogging/log_shipping/shipping.py", "line": 601, "logger": "gosilent.vpn_server.app logger"} GoSilent Cube: 2025-12-11 10:13:17 ERROR Could not find the local issuer CA with 9acd0308 (Status code (4031) :: CA chain was not found.) client_framework 1 /home/kesalaadmin/client_framework/common/gslogging/log_shipping/shipping.py 502 gosilent.client_framework.app logger 2025-12-11 10:13:17 ERROR Could not retrieve the local issuer CA object of the server certificate from 10.1.2.117:6514 (Status code (4031) :: CA chain was not found.) client_framework 1
FCS_TLSS_EXT.1	GoSilent Server: 2025-08-07T08:36:11.417347-04:00 10.1.5.12 {"program":"nginx_error","message":"2025/08/07-08:36:23 [info] 5795#5795: *2639 SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking, client: 10.1.4.67, server: 10.1.5.151:443","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","date":"2025-08-07T08:36:23-04:00"}

Associated Requirement	Example Logs
	GoSilent Cube: 2025/11/10 09:24:51 [info] 2065#2065: *27 SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking, client: 10.1.3.74, server: 0.0.0.0:443
FFW_RUL_EXT.1	GoSilent Server: 2026-02-23T15:56:29-05:00 silent-edge-enterprise kernel[]: kernel: OUT_ICMP_REJECT: IN= OUT=eth1 SRC=10.1.4.147 DST=10.1.4.67 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=60228 PROTO=ICMP TYPE=0 CODE=0 ID=33 SEQ=1489 Sep 24 09:42:10 10.1.5.155 {"program":"kernel","message":"[firewall_custom_log] ACCEPT:IN=eth1 OUT=eth0 MAC=52:54:00:49:c6:f8:00:50:56:8b:61:bd:08:00 SRC=10.1.4.93 DST=10.1.2.76 LEN=33 TOS=0x00 PREC=0x00 TTL=63 ID=17929 DF PROTO=UDP SPT=2121 DPT=4321 LEN=13 ","logtype":"iptables","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","date":"2025-09-24T05:42:10-04:00"} Oct 30 13:51:29 10.1.3.33 {"program":"kernel","message":"[firewall_custom_log] ACCEPT:IN=eth1 OUT=eth0 MAC=52:54:00:0b:0a:6a:00:50:56:8b:61:bd:08:00 SRC=10.1.4.93 DST=10.1.3.147 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=1 PROTO=TCP SPT=1234 DPT=4321 WINDOW=8192 RES=0x00 ACK URGP=0 ","logtype":"iptables","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","date":"2025-10-30T09:51:29-04:00"}
FIA_AFL.1	GoSilent Server: 2025-08-06 12:11:42 INFO Attempting to login from origin ip (10.1.3.169) and username (acumensec) core_server 1 /srv/core/./app/console_user/console_user_api.py 46 gosilent.core_server.app logger 2025-08-06 12:11:42 ERROR Failed to login, origin ip (10.1.3.169) and username (acumensec), (4084) Could not login console user core_server 0 /srv/core/./app/console_user/console_user_api.py 167 gosilent.core_server.app logger 2025-08-06 12:11:45 INFO Attempting to login from origin ip (10.1.3.169) and username (acumensec) core_server 1 /srv/core/./app/console_user/console_user_api.py 46 gosilent.core_server.app logger 2025-08-06 12:11:45 ERROR User is currently locked for a total time interval of 60s, (4081) Too many failed login attempts. Please try again later. core_server 0 /srv/core/./app/console_user/console_user_api.py 153 gosilent.core_server.app logger GoSilent Cube: 2025-10-20 19:52:41 INFO ***** Login attempted ***** client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 49 gosilent.client_framework.app logger

Associated Requirement	Example Logs
	2025-10-20 19:52:42 ERROR Failed to login (IP: 10.1.3.169, username: acumensec): User is currently locked for a total time interval of 60s. client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 93 gosilent.client_framework.app logger
FIA_UIA_EXT.1	GoSilent Server: 2025-08-06 16:57:30 INFO Attempting to login from origin ip (10.1.3.169) and username (acumensec) core_server 1 /srv/core/./app/console_user/console_user_api.py 46 gosilent.core_server.app logger 2025-08-06 16:57:31 INFO Successfully logged in from origin ip (10.1.3.169) and username (acumensec) (id:7, username:acumensec) 1 /srv/core/./app/console_user/console_user_api.py 199 gosilent.core_server.app logger GoSilent Cube: "2025-10-15 16:11:27 INFO Logged in successfully (IP: 10.1.5.106, username: Tester) client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 110 gosilent.client_framework.app logger",
FIA_X509_EXT.1/ ITT	**Unsuccessful Validation** GoSilent Server: 2025-12-12T16:06:01-0500 13[LIB] OpenSSL X.509 parsing failed 2025-12-12T16:06:01-0500 13[LIB] building CRED_CERTIFICATE - X509 failed, tried 4 builders {"timestamp": "2025-09-11 04:30:15", "type": "ERROR", "msg": "Certificate with common name (10.1.5.62) has expired : certificate expiration date (2022-08-07 07:10:00)", "user": "(id:6, username:admin)", "userid": "1", "file": "/srv/core/./common/certificate/certs.py", "line": 1555, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-09-11 04:30:15", "type": "ERROR", "msg": "Failed to verify the certificate: The certificate has expired", "user": "(id:6, username:admin)", "userid": "1", "file": "/srv/core/./common/certificate/certs.py", "line": 1949, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-09-02 07:27:13", "type": "ERROR", "msg": "Could not find the local issuer CA with 9acd0308 (Status code (4031) :: CA chain was not found.)", "user": "vpn_server", "userid": "1", "file": "/srv/vpn_edge/./common/gslogging/log_shipping/shipping.py", "line": 502, "logger": "gosilent.vpn_server.app logger"} GoSilent Cube: 2025-10-15 16:11:27 INFO Logged in successfully (IP: 10.1.5.106, username: Tester) client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 110 gosilent.client_framework.app logger

Associated Requirement	Example Logs
	Addition, Replacement or Removal of Trust Anchors GoSilent Server: {"timestamp": "2025-09-15 05:04:43", "type": "INFO", "msg": "Successfully deleted CA chain info for web console with uuid (423da0e0-8faa-11f0-8ade-000c297689e3) from (/etc/swanctl/x509ca/console/423da0e0-8faa-11f0-8ade-000c297689e3.crt)", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./common/certificate/ca_chain_index.py", "line": 252, "logger": "gosilent.core_server.app logger"} 2026-01-20 13:41:00 INFO Imported pem file ({'client_cert': None, 'ca_chain_index_info': {'uuid': '8fe751ba-f62f-11f0-83e8-52540084b611', 'common_name': 'RootCA_OCSP', 'expiration_date': '2027-01-09T17:36:00', 'hash': 'adff08dc', 'ca_contents':, 'hash_list': ['adff08dc']}, 'crl_index_info': None}) (id:6, username:admin) 1 /srv/core/./app/certificate_management/certificate_management_api.py 1354 gosilent.core_server.app logger 2026-01-20 13:41:09 INFO ***** Importing pem file initiated ***** (id:6, username:admin) 1 /srv/core/./app/certificate_management/certificate_management_api.py 717 gosilent.core_server.app logger 2026-01-20 14:12:15 INFO Successfully deleted certificate from (/etc/swanctl/x509/a18b3e54-f62f-11f0-83e8-52540084b611.crt) for certificate index with uuid (a18b3e54-f62f-11f0-83e8-52540084b611) and option (ikev2) (id:6, username:admin) 1 /srv/core/./common/certificate/certificate_index.py 1241 gosilent.core_server.app logger 2026-01-20 14:12:15 INFO Successfully deleted all certificate info with uuid (a18b3e54-f62f-11f0-83e8-52540084b611) (id:6, username:admin) 1 core/./common/certificate/certificate_index.py 1321 gosilent.core_server.app logger GoSilent Cube: 2025-12-19 09:15:09 INFO Successfully deleted CA chain info for ikev2 with uuid (df27aabd-dbdc-11f0-8d7b-000ec66c8965) from (/etc/swanctl/x509ca/df27aabd-dbdc-11f0-8d7b-000ec66c8965.1.crt) (id:1, username:admin) 1 /home/kesalaadmin/client_framework/common/certificate/ca_chain_index.py 212 gosilent.client_framework.app logger
FIA_X509_EXT.1/ Rev	**Unsuccessful Validation** GoSilent Server: 2025-08-28 06:16:23 ERROR Failed to verify a server certificate from 10.1.5.62:6514 (Status code (4114) :: The certificate does not contain the Server Auth in the Extended Key Usage field) vpn_server 1 /srv/vpn_edge/./common/gslogging/log_shipping/shipping.py 601 gosilent.vpn_server.app logger GoSilent Cube:

Associated Requirement	Example Logs
	2025-12-11 10:35:45 ERROR Certificate with common name (10.1.2.117) has expired : certificate expiration date (2024-08-07 07:10:00) client_framework 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1570 gosilent.client_framework.app logger", **Addition, Replacement or Removal of Trust Anchors** GoSilent Server: Refer to FIA_X509_EXT.1/ITT above GoSilent Cube: Refer to FIA_X509_EXT.1/ITT above
FMT_MOF.1/ManualUpdate	GoSilent Server: {"timestamp": "2025-09-15 11:49:14", "type": "INFO", "msg": "Provided service pack decompressed successfully", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/enterprise/enterprise_servicepack_utils.py", "line": 81, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-09-15 11:49:14", "type": "ERROR", "msg": "command '['openssl', 'dgst', '-sha256', '-verify', './config/attila_license_verify_pubkey.pem', '-signature', '/tmp/servicepack/overlay.sig', '/tmp/servicepack/overlay.tar.gz']' returned a non '0'", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./common/crypto/sign_verify.py", "line": 165, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-09-15 11:49:14", "type": "ERROR", "msg": "Service pack has an invalid signature, overlay signature: LEIsb3i2rh5csEZUYxqgZ2bcg5239cTqm0f/2BP+Tk5Ll9dvNC7P2mJQUqfk3CTQ\\nyH0+ZuOWnAKGm+Fgl1d+Fw+YI1nN4UtTQTm6+mG01fJ6EpXQmKjHI9gklqdmOEYd\\nlMjC0ppG31VFdMX2oJBrpDZPwaq3WArhZ7NR9lEZkivpR5IXyEP7cE751KCIHTT0\\nvPq1G0rYuMoKn1UfY2UB9fm5j27D0wNu9rNTBTsWAfBaJSKW6Z3j5avJuq/wgkxM\\nM/sdWpu7OXr2MS+sC43fwX6hWPOdsdYLFGozBWOOY710q4P86OjEZ9wa27mV8yeW\\ngJOnajsEdOgNsU7Pt5EmsroQxsDEtPbwoIizFo0cwASIOlyce/mB1l9UT1j36Vdw\\nJylmPUMSNUXutaxaTwJ2uKwnZHvbWuOcpJljJlNqU9YESXJ00Kv/fAkw8zAEwO70\\nD5cDTrt4eYprvwKKuGimccjcInS/ZObTiCK4B+7gCelAeh5VA66u/4LABJXgT0jT\\n/W+/+ChWMZ0M9V0nobnFBWoDTDf0lyPBHAsCcMz85EPu9m/pLJMXs80po/j8cU2y\\nHhizfnO5VXBlCSMSEd47XwOb7wxCk5r79J8kbdUkj7am5dE4HAzYs4JAAUmlY8R1\\nHqgQQKJWwa8MLBW3/l/ZunUnHdwDLjfljF/3jO5e9eU=\\n", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/enterprise/enterprise_servicepack_utils.py", "line": 49, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-09-15 15:17:00", "type": "INFO", "msg": "Provided service pack decompressed successfully", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/enterprise/enterprise_servicepack_utils.py", "line": 81, "logger": "gosilent.core_server.app logger"}

Associated Requirement	Example Logs
	GoSilent Cube: 2025-11-10 08:00:32 INFO Fetching update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 449 gosilent.client_framework.app logger 2025-11-10 08:00:32 INFO Successfully fetched update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 459 gosilent.client_framework.app logger
FMT_SMF.1	GoSilent Server: **Ability to administer the TOE remotely** {"timestamp": "2025-08-21 15:49:20", "type": "INFO", "msg": "***** Clicked the acknowledgement (IP: 10.1.5.106) *****", "user": "core_server", "userid": "1", "file": "/srv/core/./app/admin_console/admin_console_api.py", "line": 38, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-08-21 15:49:38", "type": "INFO", "msg": "Attempting to login from origin ip (10.1.5.106) and username (acumensec)", "user": "core_server", "userid": "1", "file": "/srv/core/./app/console_user/console_user_api.py", "line": 46, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-08-21 15:49:38", "type": "INFO", "msg": "Successfully logged in from origin ip (10.1.5.106) and username (acumensec)", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/console_user/console_user_api.py", "line": 199, "logger": "gosilent.core_server.app logger"} **Ability to configure the access banner** 2025-09-23 17:18:28 INFO Successfully updated default system setting with key (admin_console.login.banner.enabled) with value of (True) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger **Ability to configure the remote session inactivity time before session termination** 2025-09-24 15:10:00 INFO Successfully updated default system setting with key (admin_console.session.inactivity.interval) with value of (60) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger **Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates** {"timestamp": "2025-09-15 11:49:14", "type": "INFO", "msg": "Provided service pack decompressed successfully", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/enterprise/enterprise_servicepack_utils.py", "line": 81, "logger": "gosilent.core_server.app logger"}

Associated Requirement	Example Logs
	Ability to start and stop services; 2026-03-11 14:29:43 INFO Successfully updated default system setting with key (logging.shipping.enabled) with value of (True) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger 2026-03-11 14:29:43 INFO Successfully updated default system setting with key (logging.destination.url) with value of (10.1.5.62) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger {"timestamp": "2025-09-10 15:07:59", "type": "INFO", "msg": "Successfully updated default system setting with key (logging.shipping.enabled) with value of (False)", "user": "(id:6, username:admin)", "userid": "1", "file": "/srv/core/./models/system_setting/system_setting_controller.py", "line": 236, "logger": "gosilent.core_server.app logger"} **Ability to modify the behaviour of the transmission of audit data to an external IT entity;** 2026-03-11 14:29:43 INFO Successfully updated default system setting with key (logging.shipping.enabled) with value of (True) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger 2026-03-11 14:29:43 INFO Successfully updated default system setting with key (logging.destination.url) with value of (10.1.5.62) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger **Ability to manage the cryptographic keys** 2026-02-16 22:15:17 INFO ***** Importing pem file initiated ***** (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/api/certificate_management/certificate_management_api.py 547 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Trying to load the key from DER encoded data (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 238 gosilent.client_framework.app logger 2026-02-16 22:15:17 ERROR Could not validate a private key password because : (Could not deserialize key data.) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 370 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Trying to load the key from DER encoded data (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 238 gosilent.client_framework.app logger 2026-02-16 22:15:17 ERROR Failed to load key data: Could not deserialize key data. (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 275 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10,

Associated Requirement	Example Logs
	username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying CA certificate (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2020 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Certificate with common name (ICA1_OCSP) has a valid date : certificate expiration date (2026-09-10 15:24:00) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1578 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully verified CA certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2046 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying EC curve in intermediate CA (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2061 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying CA certificate (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2020 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Certificate with common name (ICA1_OCSP) has a valid date : certificate expiration date (2026-09-10 15:24:00) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1578 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully verified CA certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2046 gosilent.client_framework.app logger **Ability to configure the cryptographic functionality** 2026-01-30T18:12:51+0000 16[IKE] initiating IKE_SA profile-1-cn[32] to 10.1.4.67 2026-01-30T18:12:51+0000 16[ENC] generating IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP)] 2026-01-30T18:12:51+0000 16[NET] sending packet: from 10.1.4.187[500] to 10.1.4.67[500] (368 bytes) 2026-01-30T18:12:51+0000 06[NET] received packet: from 10.1.4.67[500] to 10.1.4.187[500] (36 bytes) 2026-01-30T18:12:51+0000 06[ENC] parsed IKE_SA_INIT response 0 [N(NO_PROP)] 2026-01-30T18:12:51+0000 06[IKE] received NO_PROPOSAL_CHOSEN notify error

Associated Requirement	Example Logs
	Ability to configure the lifetime for IPsec SAs 2026-01-30T23:29:57+0000 01[IKE] establishing CHILD_SA profile-3-san{2} 2026-01-30T23:29:57+0000 01[ENC] generating IKE_AUTH request 1 [IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH CPRQ(ADDR DNS) SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP)] 2026-01-30T23:29:57+0000 01[ENC] splitting IKE message (1306 bytes) into 2 fragments 2026-01-30T23:29:57+0000 01[ENC] generating IKE_AUTH request 1 [EF(1/2)] 2026-01-30T23:29:57+0000 01[ENC] generating IKE_AUTH request 1 [EF(2/2)] 2026-01-30T23:29:57+0000 01[NET] sending packet: from 10.1.4.187[4500] to 10.1.4.147[4500] (1248 bytes) 2026-01-30T23:29:57+0000 01[NET] sending packet: from 10.1.4.187[4500] to 10.1.4.147[4500] (123 bytes) 2026-01-30T23:29:57+0000 09[NET] received packet: from 10.1.4.147[4500] to 10.1.4.187[4500] (991 bytes) 2026-01-30T23:29:57+0000 09[ENC] parsed IKE_AUTH response 1 [IDr CERT AUTH CPRP(ADDR DNS DNS) SA TSi TSr] **Ability to configure the list of supported (D)TLS ciphers** 2026-03-11 15:23:26 INFO Successfully updated default system setting with key (logging.shipping.tls.cipher.id) with value of (4) (id:7, username:acumensec) 1 /srv/core/./models/system_setting/system_setting_controller.py 236 gosilent.core_server.app logger **Ability to configure the interaction between TOE components** 2025-10-22T16:46:37-0400 09[CFG] selected proposal: ESP:AES_GCM_16_256/NO_EXT_SEQ 2025-10-22T16:46:37-0400 09[IKE] CHILD_SA 10-1-4-222{72} established with SPIs cc38f6d4_i 89d06e9a_o and TS 0.0.0.0/0 === 172.16.184.1/32 2025-10-22T16:46:37-0400 09[ENC] generating IKE_AUTH response 1 [IDr CERT AUTH CPRP(ADDR DNS DNS) SA TSi TSr] 2025-10-22T16:46:37-0400 09[NET] sending packet: from 10.1.4.147[4500] to 10.1.4.222[4500] (926 bytes) **Ability to set the time which is used for time-stamps** 2025-10-15 17:19:12 INFO ***** Setting system time initiated ***** (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/api/date_and_time/date_and_time_api.py 43 gosilent.client_framework.app logger **Ability to configure the reference identifier for the peer** 2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: Certificate subject does not match configured hostname; hostname='10.1.2.117', certificate='10.1.2.111' 2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: SSL error while writing stream; tls_error='error:0A000086:SSL routines::certificate verify failed', location='/etc/syslog-ng/syslog-ng.conf:294:5'

Associated Requirement	Example Logs
	2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: I/O error occurred while writing; fd='38', error='Broken pipe (32)' 2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: Syslog connection broken; fd='38', server='AF_INET(10.1.2.117:6514)', time_reopen='300' **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors** 2026-02-16 22:15:17 INFO ***** Importing pem file initiated ***** (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/api/certificate_management/certificate_management_api.py 547 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Trying to load the key from DER encoded data (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 238 gosilent.client_framework.app logger 2026-02-16 22:15:17 ERROR Could not validate a private key password because : (Could not deserialize key data.) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 370 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Trying to load the key from DER encoded data (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 238 gosilent.client_framework.app logger 2026-02-16 22:15:17 ERROR Failed to load key data: Could not deserialize key data. (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 275 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying CA certificate (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2020 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Certificate with common name (ICA1_OCSP) has a valid date : certificate expiration date (2026-09-10 15:24:00) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1578 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully verified CA certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2046 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying EC curve in intermediate CA (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2061 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying CA certificate (id:10, username:acumensec) 1

Associated Requirement	Example Logs
	/home/kesalaadmin/client_framework/common/certificate/certs.py 2020 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Certificate with common name (ICA1_OCSP) has a valid date : certificate expiration date (2026-09-10 15:24:00) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1578 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully verified CA certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2046 gosilent.client_framework.app logger **Ability to generate Certificate Signing Request (CSR) and process CA certificate response** 2026-03-12 12:24:13 INFO Creating a CSR ({'common_name': '10.1.4.149_1', 'cert_uuid': '/tmp/e87790a6-1e2f-11f1-95ea-000c29f1e84e/CSR-e87790a6-1e2f-11f1-95ea-000c29f1e84e'}) (id:7, username:acumensec) 1 /srv/core/./common/certificate/certs.py 477 gosilent.core_server.app logger 2026-03-12 12:24:13 INFO CSR SAN data\\nDNS.1=10.1.4.149_1\\n (id:7, username:acumensec) 1 /srv/core/./common/certificate/certs.py 526 gosilent.core_server.app logger 2026-03-12 12:24:14 INFO Successfully created CSR from config (/tmp/tmpy18_swnn/tmpzdlxnv0c) cert_info ({'common_name': '10.1.4.149_1', 'cert_uuid': '/tmp/e87790a6-1e2f-11f1-95ea-000c29f1e84e/CSR-e87790a6-1e2f-11f1-95ea-000c29f1e84e'}) (id:7, username:acumensec) 1 /srv/core/./common/certificate/certs.py 547 gosilent.core_server.app logger **Ability to administer the TOE locally** 2025-10-16 16:43:20 INFO ***** Login attempted ***** client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 49 gosilent.client_framework.app logger 2025-10-16 16:43:20 INFO Logged in successfully (IP: 192.168.128.54, username: acumensec) client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 110 gosilent.client_framework.app logger **Ability to configure the local session inactivity time before session termination or locking** 2025-10-23 16:49:25 INFO Logged out automatically because of inactivity (IP: 192.168.128.54, username: acumensec) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/app/core_a **Ability to configure the authentication failure parameters for FIA_AFL.1** /home/kesalaadmin/client_framework/app/kesala_users.py 49 gosilent.client_framework.app logger", "2025-10-20 19:52:42 ERROR Failed to login (IP: 10.1.3.169, username: acumensec): User is currently locked for a total

Associated Requirement	Example Logs
	time interval of 60s. client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 93 gosilent.client_framework.app logger GoSilent Cube: **Ability to administer the TOE remotely** 2025-10-21 16:50:17 INFO ***** Clicked the acknowledgement (IP: 10.1.3.169) ***** client_framework 1 2025-10-21 16:50:27 INFO ***** Login attempted ***** client_framework 1 2025-10-21 16:50:27 INFO Getting system settings client_framework 1 2025-10-21 16:50:27 INFO Logged in successfully (IP: 10.1.3.169, username: admin) client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 110 gosilent.client_framework.app logger", **Ability to configure the access banner** 2026-03-12 17:03:34 INFO System setting (client.login.banner.enabled) has changed, updating to (True) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/app/system_settings/system_settings.py 175 gosilent.client_framework.app logger **Ability to configure the remote session inactivity time before session termination** 2025-10-23 16:07:54 INFO Logged out automatically because of inactivity (IP: 192.168.128.54, username: acumensec) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/app/core_app.py 116 gosilent.client_framework.app logger **Ability to update the** 1 **TOE, and to verify the updates using digital signature capability prior to installing those updates** 2025-11-10 08:00:32 INFO Fetching update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 449 gosilent.client_framework.app logger 2025-11-10 08:00:32 INFO Successfully fetched update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 459 gosilent.client_framework.app logger 2025-11-10 08:00:32 INFO current update.json is up to date client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 420 gosilent.client_framework.app logger

Associated Requirement	Example Logs
	2025-11-10 08:00:32 INFO up to date already (26.01.1.007) client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 153 gosilent.client_framework.app logger 2025-11-10 08:12:48 INFO OTA update was performed successfully. Restoring settings. ota 1 /home/kesalaadmin/client_framework/first_boot_after_update_runner.py 145 gosilent.ota.pre_scripts_log 2025-11-10 08:12:49 INFO Successfully updated from version 26.01.1.005 to version 26.01.1.007 ota 1 /home/kesalaadmin/client_framework/pre_scripts/successful_update_log.py 15 gosilent.ota.pre_scripts_log **Ability to start and stop services** 2026-03-12 17:01:23 INFO Enabling log shipping... (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/gslogging/log_shipping/shipping.py 137 gosilent.client_framework.app logger 2026-03-12 17:01:19 INFO Disabling log shipping... (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/gslogging/log_shipping/shipping.py 119 gosilent.client_framework.app logger **Ability to modify the behaviour of the transmission of audit data to an external IT entity** 2026-03-12 17:01:23 INFO Enabling log shipping... (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/gslogging/log_shipping/shipping.py 137 gosilent.client_framework.app logger **Ability to manage the cryptographic keys** 2026-02-16 22:15:17 INFO ***** Importing pem file initiated ***** (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/api/certificate_management/certificate_management_api.py 547 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Trying to load the key from DER encoded data (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 238 gosilent.client_framework.app logger 2026-02-16 22:15:17 ERROR Could not validate a private key password because : (Could not deserialize key data.) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 370 gosilent.client_framework.app logger

Associated Requirement	Example Logs
	2026-02-16 22:15:17 INFO Trying to load the key from DER encoded data (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 238 gosilent.client_framework.app logger 2026-02-16 22:15:17 ERROR Failed to load key data: Could not deserialize key data. (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 275 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying CA certificate (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2020 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Certificate with common name (ICA1_OCSP) has a valid date : certificate expiration date (2026-09-10 15:24:00) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1578 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully verified CA certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2046 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying EC curve in intermediate CA (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2061 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Verifying CA certificate (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2020 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Certificate with common name (ICA1_OCSP) has a valid date : certificate expiration date (2026-09-10 15:24:00) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1578 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully validated basic contraints for certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1676 gosilent.client_framework.app logger 2026-02-16 22:15:17 INFO Successfully verified CA certificate with common name (ICA1_OCSP) (id:10, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2046 gosilent.client_framework.app logger

Associated Requirement	Example Logs
	Ability to configure the cryptographic functionality 2026-01-30T18:12:51+0000 16[IKE] initiating IKE_SA profile-1-cn[32] to 10.1.4.67 2026-01-30T18:12:51+0000 16[ENC] generating IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP)] 2026-01-30T18:12:51+0000 16[NET] sending packet: from 10.1.4.187[500] to 10.1.4.67[500] (368 bytes) 2026-01-30T18:12:51+0000 06[NET] received packet: from 10.1.4.67[500] to 10.1.4.187[500] (36 bytes) 2026-01-30T18:12:51+0000 06[ENC] parsed IKE_SA_INIT response 0 [N(NO_PROP)] 2026-01-30T18:12:51+0000 06[IKE] received NO_PROPOSAL_CHOSEN notify error **Ability to configure the lifetime for IPsec SAs** 2026-01-31T23:25:12+0000 08[ENC] parsed INFORMATIONAL request 1 [D] 2026-01-31T23:25:12+0000 08[IKE] received DELETE for ESP CHILD_SA with SPI c71a01ca 2026-01-31T23:25:12+0000 08[IKE] closing CHILD_SA profile-3-san{4} with SPIs 2de5a33e_i (0 bytes) c71a01ca_o (0 bytes) and TS 172.16.184.1/32 === 10.1.4.0/24 172.16.176.0/24 2026-01-31T23:25:12+0000 08[IKE] sending DELETE for ESP CHILD_SA with SPI 2de5a33e 2026-01-31T23:25:12+0000 08[IKE] outbound CHILD_SA profile-3-san{5} established with SPIs 20399f09_i c1d42766_o and TS 172.16.184.1/32 === 10.1.4.0/24 172.16.176.0/24 2026-01-31T23:25:12+0000 08[IKE] rekeyed CHILD_SA profile-3-san{4} with SPIs 2de5a33e_i c71a01ca_o with profile-3-san{5} with SPIs 20399f09_i c1d42766_o 2026-01-31T23:25:12+0000 08[IKE] delay closing of inbound CHILD_SA profile-3-san{4} for 5s 2026-01-31T23:25:12+0000 08[ENC] generating INFORMATIONAL response 1 [D] 2026-01-31T23:25:12+0000 08[NET] sending packet: from 10.1.4.187[4500] to 10.1.4.147[4500] (69 bytes) **Ability to configure the list of supported (D)TLS ciphers** 2026-03-11 19:25:42 INFO System setting (logging.shipping.tls.cipher) has changed, updating to (TLS_AES_256_GCM_SHA384) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/app/system_settings/system_settings.py 175 gosilent.client_framework.app logger

Associated Requirement	Example Logs
	Ability to ITT **configure the interaction between TOE components** 2025-10-22T19:52:05+0000 14[IKE] IKE_SA profile-1-san[7] established between 10.1.4.222[10.1.4.222]...10.1.4.147[10.1.4.147] 2025-10-22T19:52:05+0000 14[IKE] scheduling rekeying in 13227s 2025-10-22T19:52:05+0000 14[IKE] maximum IKE_SA lifetime 14667s 2025-10-22T19:52:05+0000 14[CFG] selected proposal: ESP:AES_GCM_16_256/NO_EXT_SEQ 2025-10-22T19:52:05+0000 14[IKE] CHILD_SA profile-1-san{5} established with SPIs 89d06e9a_i cc38f6d4_o and TS 172.16.184.1/32 === 0.0.0.0/0 **Ability to set the time which is used for time-stamps** 2025-10-15 17:19:12 INFO ***** Setting system time initiated ***** (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/api/date_and_time/date_and_time_api.py 43 gosilent.client_framework.app logger **Ability to configure the reference identifier for the peer** 2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: Certificate subject does not match configured hostname; hostname='10.1.2.117', certificate='10.1.2.111' 2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: SSL error while writing stream; tls_error='error:0A000086:SSL routines::certificate verify failed', location='/etc/syslog-ng/syslog-ng.conf:294:5' 2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: I/O error occurred while writing; fd='38', error='Broken pipe (32)' 2025-12-05T09:56:59+00:00 gosilent syslog-ng[3201]: syslog-ng[3201]: Syslog connection broken; fd='38', server='AF_INET(10.1.2.117:6514)', time_reopen='300' **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors** "2026-04-08 14:58:07 INFO ***** Importing pem file initiated ***** (id:1, username:admin) 1 /home/kesalaadmin/client_framework/api/certificate_management/certificate_management_api.py 547 gosilent.client_framework.app logger",

Associated Requirement	Example Logs
	"2026-04-08 14:58:07 INFO Verifying CA certificate (id:1, username:admin) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2020 gosilent.client_framework.app logger", "2026-04-08 14:58:07 INFO Successfully verified CA certificate with common name (AF-RootCA) (id:1, username:admin) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 2046 gosilent.client_framework.app logger", **Ability to generate Certificate Signing Request (CSR) and process CA certificate response** 2026-03-12 17:48:29 INFO ***** Creating a CSR initiated ({'common_name': '10.1.4.187_1', 'cert_uuid': 'adf677c2-1e3b-11f1-947a-000ec66c8965'}) ***** (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/api/certificate_management/certificate_management_api.py 87 gosilent.client_framework.app logger 2026-03-12 17:48:29 INFO Attempting to create private key with curve name (secp384r1) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 91 gosilent.client_framework.app logger 2026-03-12 17:48:29 INFO Successfully created private key with curve name (secp384r1) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 135 gosilent.client_framework.app logger 2026-03-12 17:48:29 INFO Successfully copied over private key from (/tmp/adf677c2-1e3b-11f1-947a-000ec66c8965/KEY-adf677c2-1e3b-11f1-947a-000ec66c8965) to (/etc/swanctl/private/adf677c2-1e3b-11f1-947a-000ec66c8965.key) with uuid (adf677c2-1e3b-11f1-947a-000ec66c8965) for option (ikev2) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/certificate/certificate_index.py 610 gosilent.client_framework.app logger 2026-03-12 17:48:29 INFO Zeroizing out all files in /tmp/adf677c2-1e3b-11f1-947a-000ec66c8965 (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/utils/file_utils.py 378 gosilent.client_framework.app logger 2026-03-12 17:48:29 INFO Attempting to zeroize out file (/tmp/adf677c2-1e3b-11f1-947a-000ec66c8965/KEY-adf677c2-1e3b-11f1-947a-000ec66c8965) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/utils/file_utils.py 316 gosilent.client_framework.app logger 2026-03-12 17:48:30 INFO Zeroized out file (/tmp/adf677c2-1e3b-11f1-947a-000ec66c8965/KEY-adf677c2-1e3b-11f1-947a-000ec66c8965) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/utils/file_utils.py 352 gosilent.client_framework.app logger 2026-03-12 17:48:30 INFO Done zeroizing out all files in /tmp/adf677c2-1e3b-11f1-947a-000ec66c8965 - Deleted? True (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/common/utils/file_utils.py 412 gosilent.client_framework.app logger

Associated Requirement	Example Logs
	Ability to administer the TOE locally 2025-10-16 16:43:20 INFO ***** Login attempted ***** client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 49 gosilent.client_framework.app logger 2025-10-16 16:43:20 INFO Getting system settings client_framework 1 /home/kesalaadmin/client_framework/app/system_settings/system_settings.py 55 gosilent.client_framework.app logger 2025-10-16 16:43:20 INFO Logged in successfully (IP: 192.168.128.54, username: acumensec) client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 110 gosilent.client_framework.app logger **Ability to configure the local session inactivity time before session termination or locking** 2025-10-23 16:07:54 INFO Logged out automatically because of inactivity (IP: 192.168.128.54, username: acumensec) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/app/core_app.py 116 gosilent.client_framework.app logger **Ability to configure the authentication failure parameters for FIA_AFL.1** 2025-10-20 19:52:42 ERROR Failed to login (IP: 10.1.3.169, username: acumensec): User is currently locked for a total time interval of 60s. client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 93 gosilent.client_framework.app logger
FMT_SMF.1/FFW	GoSilent Server: Sep 19 08:36:44 10.1.5.155 {"user":"(id:6, username:admin)","program":"gosilent","message":"Got the advanced firewall rules for ipv4 (number of lines: 73)","logger":"gosilent.core_server.firewall log","line":"233","level":"INFO","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","file":"/srv/core/./app/firewall/firewall_api.py","facility":"user","date":"2025-09-19 04:36:56"}
FMT_SMF.1/VPN	GoSilent Server: Sep 19 08:36:44 10.1.5.155 {"user":"(id:6, username:admin)","program":"gosilent","message":"Got the advanced firewall rules for ipv4 (number of lines: 73)","logger":"gosilent.core_server.firewall log","line":"233","level":"INFO","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","file":"/srv/core/./app/firewall/firewall_api.py","facility":"user","date":"2025-09-19 04:36:56"}

Associated Requirement	Example Logs
	Sep 19 08:36:44 10.1.5.155 {"user":"(id:6, username:admin)","program":"gosilent","message":"Successfully retrieved firewall profile (default-custom) for the interface (all)","logger":"gosilent.core_server.firewall log","line":"262","level":"INFO","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","file":"/srv/core/./common/firewall/firewall.py","facility":"user","date":"2025-09-19 04:36:56"}
FPF_RUL_EXT.1	GoSilent Server: Sep 24 09:42:10 10.1.5.155 {"program":"kernel","message":"[firewall_custom_log] ACCEPT:IN=eth1 OUT=eth0 MAC=52:54:00:49:c6:f8:00:50:56:8b:61:bd:08:00 SRC=10.1.4.93 DST=10.1.2.76 LEN=33 TOS=0x00 PREC=0x00 TTL=63 ID=17929 DF PROTO=UDP SPT=2121 DPT=4321 LEN=13 ","logtype":"iptables","host":"e88af2e1-264b-11e9-8a98-6a00008c5330","date":"2025-09-24T05:42:10-04:00"}
FPT_ITT.1	**Initiation of the Trusted Channel** GoSilent Server: 2026-02-10T14:22:15-0500 16[NET] received packet: from 10.1.4.187[500] to 10.1.4.149[500] (368 bytes) 2026-02-10T14:22:15-0500 16[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP)] 2026-02-10T14:22:15-0500 16[IKE] 10.1.4.187 is initiating an IKE_SA 2025-10-22T16:46:37-0400 09[CFG] selected proposal: ESP:AES_GCM_16_256/NO_EXT_SEQ 2025-10-22T16:46:37-0400 09[IKE] CHILD_SA 10-1-4-222{72} established with SPIs cc38f6d4_i 89d06e9a_o and TS 0.0.0.0/0 === 172.16.184.1/32 2025-10-22T16:46:37-0400 09[ENC] generating IKE_AUTH response 1 [IDr CERT AUTH CPRP(ADDR DNS DNS) SA TSi TSr] 2025-10-22T16:46:37-0400 09[NET] sending packet: from 10.1.4.147[4500] to 10.1.4.222[4500] (926 bytes) GoSilent Cube: 2025-12-19T08:56:54+0000 09[IKE] initiating IKE_SA profile-1-san[2] to 10.1.4.115 2025-12-19T08:56:54+0000 09[ENC] generating IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP)] 2025-12-19T08:56:54+0000 09[NET] sending packet: from 10.1.4.187[500] to 10.1.4.115[500] (368 bytes)

Associated Requirement	Example Logs
	Termination of the Trusted Channel GoSilent Server: 2026-02-10T14:43:10-0500 03[IKE] no IKE config found for 10.1.4.149...10.1.4.187, sending NO_PROPOSAL_CHOSEN 2026-01-29T12:20:48-0500 06[IKE] deleting IKE_SA 10-1-4-187[8] between 10.1.4.147[10.1.4.147]...10.1.4.187[10.1.4.187] 2026-01-29T12:20:48-0500 06[IKE] IKE_SA deleted GoSilent Cube: 2025-12-19T08:56:54+0000 08[ENC] generating INFORMATIONAL request 2 [N(AUTH_FAILED)] **Failure of the Trusted Channel** GoSilent Server: 2025-09-26T14:27:52-0400 08[IKE] IKE_SA 10-1-4-67[21] established between 10.1.4.149 [10.1.4.149]...10.1.4.67[10.1.4.67] 2025-09-26T14:27:52-0400 08[CFG] received proposals: ESP:AES_CBC_128/AES_CBC_192/AES_CBC_256/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/HMAC_SHA1_96/AES_XCBC_96/NO_EXT_SEQ, ESP:AES_GCM_16_128/AES_GCM_16_192/AES_GCM_16_256", 2025-09-26T14:27:52-0400 08[CFG] configured proposals: ESP:AES_GCM_16_256/ECP_384/NO_EXT_SEQ 2025-09-26T14:27:52-0400 08[IKE] no acceptable proposal found 2025-09-26T14:27:52-0400 08[IKE] failed to establish CHILD_SA, keeping IKE_SA GoSilent Cube: 2025-12-19T08:56:54+0000 08[CFG] subject certificate invalid (valid from Sep 10 15:47:00 2024 to Sep 10 15:24:00 2024) 2025-12-19T08:56:54+0000 08[IKE] no trusted ECDSA public key found for '10.1.4.115'
FPT_STM_EXT.1	GoSilent Server: "timestamp": "2025-10-07 07:11:00", "type": "INFO", "msg": "Successfully set the system date and time", "user": "(id:6, username:admin)", "userid": "1", "file": "/srv/core/./common/system/system_management.py", "line": 221, "logger": "gosilent.core_server.system log"} {"timestamp": "2025-10-07 07:11:00", "type": "INFO", "msg": "Getting system date and time", "user": "(id:6, username:admin)", "userid": "1", "file": "/srv/core/./common/system/system_management.py", "line": 90, "logger": "gosilent.core_server.system log"}

Associated Requirement	Example Logs
	{"timestamp": "2025-10-07 07:11:00", "type": "INFO", "msg": "time and date: 2025-10-07T11:11", "user": "(id:6, username:admin)", "userid": "1", "file": "/srv/core/./common/system/system_management.py", "line": 102, "logger": "gosilent.core_server.system log"} GoSilent Cube: 2025-10-15 17:19:12 INFO ***** Setting system time initiated ***** (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/api/date_and_time/date_and_time_api.py 43 gosilent.client_framework.app logger
FPT_TUD_EXT.1	GoSilent Server: {"timestamp": "2025-09-15 11:49:14", "type": "INFO", "msg": "Provided service pack decompressed successfully", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/enterprise/enterprise_servicepack_utils.py", "line": 81, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-09-15 11:49:14", "type": "ERROR", "msg": "command '['openssl', 'dgst', '-sha256', '-verify', './config/attila_license_verify_pubkey.pem', '-signature', '/tmp/servicepack/overlay.sig', '/tmp/servicepack/overlay.tar.gz']' returned a non '0'", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./common/crypto/sign_verify.py", "line": 165, "logger": "gosilent.core_server.app logger"} {"timestamp": "2025-09-15 11:49:14", "type": "ERROR", "msg": "Service pack has an invalid signature, overlay signature: LEIsb3i2rh5csEZUYxqgZ2bcg5239cTqm0f/2BP+Tk5Ll9dvNC7P2mJQUqfk3CTQ\\nyH0+ZuOWnAKGm+Fgl1d+Fw+YI1nN4UtTQTm6+mG01fJ6EpXQmKjHI9gklqdmOEYd\\nlMjC0ppG31VFdMX2oJBrpDZPwaq3WArhZ7NR9lEZkivpR5IXyEP7cE751KCIHTT0\\nvPq1G0rYuMoKn1UfY2UB9fm5j27D0wNu9rNTBTsWAfBaJSKW6Z3j5avJuq/wgkxM\\nM/sdWpu7OXr2MS+sC43fwX6hWPOdsdYLFGozBWOOY710q4P86OjEZ9wa27mV8yeW\\ngJOnajsEdOgNsU7Pt5EmsroQxsDEtPbwoIizFo0cwASIOlyce/mB1l9UT1j36Vdw\\nJylmPUMSNUXutaxaTwJ2uKwnZHvbWuOcpJljJlNqU9YESXJ00Kv/fAkw8zAEwO70\\nD5cDTrt4eYprvwKKuGimccjcInS/ZObTiCK4B+7gCelAeh5VA66u/4LABJXgT0jT\\n/W+/+ChWMZ0M9V0nobnFBWoDTDf0lyPBHAsCcMz85EPu9m/pLJMXs80po/j8cU2y\\nHhizfnO5VXBlCSMSEd47XwOb7wxCk5r79J8kbdUkj7am5dE4HAzYs4JAAUmlY8R1\\nHqgQQKJWwa8MLBW3/l/ZunUnHdwDLjfljF/3jO5e9eU=\\n", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/enterprise/enterprise_servicepack_utils.py", "line": 49, "logger": "gosilent.core_server.app logger"} GoSilent Cube: "2025-11-10 08:00:32 INFO Fetching update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 449 gosilent.client_framework.app logger",

Associated Requirement	Example Logs
	"2025-11-10 08:00:32 INFO Successfully fetched update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 459 gosilent.client_framework.app logger",
FTA_SSL.3	GoSilent Server: 2025-08-20 14:33:12 INFO User (7) was auto logged out, origin ip (10.1.3.169) (id:7, username:acumensec) 1 /srv/core/./app/console_user/console_user_api.py 222 gosilent.core_server.app logger GoSilent Cube: "2025-10-23 17:40:17 INFO Logged out automatically because of inactivity (IP: 10.1.3.169, username: acumensec) (id:2, username:acumensec) 1 /home/kesalaadmin/client_framework/app/core_app.py 116 gosilent.client_framework.app logger",
FTA_SSL.4	GoSilent Server: {"timestamp": "2025-08-20 15:42:54", "type": "INFO", "msg": "User (7) is logging out, origin ip (10.1.3.169)", "user": "(id:7, username:acumensec)", "userid": "1", "file": "/srv/core/./app/console_user/console_user_api.py", "line": 210, "logger": "gosilent.core_server.app logger"} GoSilent Cube: 2025-11-10 08:00:32 INFO Fetching update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 449 gosilent.client_framework.app logger 2025-11-10 08:00:32 INFO Successfully fetched update.json from http://server.gosilent/gsc100/v1/update.json client_framework 1 /home/kesalaadmin/client_framework/app/scripts/ota_controller.py 459 gosilent.client_framework.app logger
FTA_SSL_EXT.1	GoSilent Server: Refer to FTA_SSL.3 above. GoSilent Cube: Refer to FTA_SSL.3 above.
FTP_ITC.1	**Initiation of the Trusted Channel** GoSilent Server:

Associated Requirement	Example Logs
	2026-02-19 14:16:00 INFO Enabling log shipping... vpn_server 1 /srv/vpn_edge/./common/gslogging/log_shipping/shipping.py 137 gosilent.vpn_server.app logger {"timestamp": "2025-09-01 09:21:13", "type": "INFO", "msg": "Successfully verified certificate with common name (*.acumensec.local)", "user": "vpn_server", "userid": "1", "file": "/srv/vpn_edge/./common/certificate/certs.py", "line": 1986, "logger": "gosilent.vpn_server.app logger"} GoSilent Cube: 2026-02-19 14:16:00 INFO Enabling log shipping... vpn_server 1 /srv/vpn_edge/./common/gslogging/log_shipping/shipping.py 137 gosilent.vpn_server.app logger **Termination of the Trusted Channel** GoSilent Server: 2025-11-05T03:01:04-05:00 silent-edge-enterprise syslog-ng[1926]: syslog-ng[1926]: I/O error occurred while writing; fd='31', error='Broken pipe (32)' GoSilent Cube: 2025-12-12 06:44:05 WARNING Disabling the log shipping... client_framework 1 /home/kesalaadmin/client_framework/common/gslogging/log_shipping/shipping.py 603 gosilent.client_framework.app logger **Failure of the Trusted Channel** GoSilent Server: {"timestamp": "2025-09-12 04:00:36", "type": "ERROR", "msg": "Failed to verify a server certificate from 10.1.5.62:6514 (Status code (4114) :: The certificate does not contain the Server Auth in the Extended Key Usage field)", "user": "vpn_server", "userid": "1", "file": "/srv/vpn_edge/./common/gslogging/log_shipping/shipping.py", "line": 601, "logger": "gosilent.vpn_server.app logger"} {"timestamp": "2025-09-09 03:23:38", "type": "ERROR", "msg": "Could not get server cert obj from URI (10.1.5.62:6514): '808B0867FC7E0000:error:0A000102:SSL routines:ssl_choose_client_version:unsupported protocol:../ssl/statem/statem_lib.c:1957:\nCONNECTED(00000003) GoSilent Cube:

Associated Requirement	Example Logs
	2025-12-12 06:44:05 ERROR Failed to verify the certificate: The certificate does not contain the Server Auth in the Extended Key Usage field client_framework 1 /home/kesalaadmin/client_framework/common/certificate/certs.py 1987 gosilent.client_framework.app logger 2025-12-12 06:44:05 ERROR Failed to verify a server certificate from 10.1.2.117:6514 (Status code (4114) :: The certificate does not contain the Server Auth in the Extended Key Usage field) client_framework 1
FTP_ITC.1/VPN	**Initiation of the Trusted Channel** GoSilent Server: "2026-02-10T14:22:15-0500 16[NET] received packet: from 10.1.4.187[500] to 10.1.4.149[500] (368 bytes)", "2026-02-10T14:22:15-0500 16[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP)]", "2026-02-10T14:22:15-0500 16[IKE] 10.1.4.187 is initiating an IKE_SA", GoSilent Cube: "2025-12-19T08:56:54+0000 09[IKE] initiating IKE_SA profile-1-san[2] to 10.1.4.115", "2025-12-19T08:56:54+0000 09[ENC] generating IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP)]", **Termination of the Trusted Channel** GoSilent Server: "2026-03-04T12:12:36-0500 13[IKE] deleting IKE_SA 10-1-4-187[26] between 10.1.4.149[10.1.4.149]...10.1.4.187[10.1.4.187]", GoSilent Cube: 2026-04-08T14:40:57+0000 13[IKE] deleting IKE_SA profile-1-san[79] between 10.1.4.187[10.1.4.187]...10.1.4.149[10.1.4.149] **Failure of the Trusted Channel** GoSilent Server: "2025-09-26T14:27:52-0400 08[CFG] configured proposals: ESP:AES_GCM_16_256/ECP_384/ NO_EXT_SEQ", "2025-09-26T14:27:52-0400 08[IKE] no acceptable proposal found", "2025-09-26T14:27:52-0400 08[IKE] failed to establish CHILD_SA, keeping IKE_SA",

Associated Requirement	Example Logs
	GoSilent Cube: "2025-12-19T08:56:54+0000 08[CFG] subject certificate invalid (valid from Sep 10 15:47:00 2024 to Sep 10 15:24:00 2024)", "2025-12-19T08:56:54+0000 08[IKE] no trusted ECDSA public key found for '10.1.4.115'",
FTP_TRP.1/Admin	**Initiation of the Trusted Path** GoSilent Server: "2026-02-26 10:29:56 INFO Successfully logged in from origin ip (10.1.5.106) and username (admin) (id:6, username:admin) 1 /srv/core/./app/console_user/console_user_api.py 199 gosilent.core_server.app logger", GoSilent Cube: "2026-04-08 14:08:34 INFO ***** Login attempted ***** client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 49 gosilent.client_framework.app logger", "2026-04-08 14:08:34 INFO Logged in successfully (IP: 10.1.3.169, username: admin) client_framework 1 /home/kesalaadmin/client_framework/app/kesala_users.py 110 gosilent.client_framework.app logger", **Termination of the Trusted Path** GoSilent Server: "2026-04-07 14:19:34 INFO User (6) is logging out, origin ip (192.168.253.123) (id:6, username:admin) 1 /srv/core/./app/console_user/console_user_api.py 210 gosilent.core_server.app logger", GoSilent Cube: "2026-04-08 14:08:26 INFO ***** Logout attempted ***** (id:1, username:admin) 1 /home/kesalaadmin/client_framework/app/core_app.py 114 gosilent.client_framework.app logger", "2026-04-08 14:08:26 INFO Logged out successfully (IP: 10.1.3.169, username: admin) (id:1, username:admin) 1 /home/kesalaadmin/client_framework/app/core_app.py 116 gosilent.client_framework.app logger", **Failure of the Trusted Path** GoSilent Server: "2026/02/18 16:49:28 [info] 1464#1464: *8 SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking, client: 10.1.4.67, server: 10.1.5.151:443",

Associated Requirement	Example Logs
	GoSilent Cube: 2025/11/10 09:24:51 [info] 2065#2065: *26 SSL_do_handshake() failed (SSL: error:0A0000C1:SSL routines::no shared cipher) while SSL handshaking, client: 10.1.3.74, server: 0.0.0.0:443