GoSilent Cube + GoSilent Server v25.01

Common Criteria Guide

Version 1.8

December 2022

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

List of Figures

No table of figures entries found.

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions and related information to achieve the Common Criteria evaluated configuration of the GoSilent Cube + GoSilent Server v25.01 TOE.

1.2 Audience

2 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 documents listed in Table 3.

1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/.

1.3.1 Conformance Claims

1.3.1.1 Common Criteria Conformance

4 The Target of Evaluation subject to this evaluation complies with the following:

a) CC Version 3.1 Revision 5

b) CC Part 2 Extended

c) CC Part 3 Conformant

1.3.1.2 Protection Profile Conformance

5 This Common Criteria evaluation was performed against the requirements of the following Protection Profiles and PP Modules:

a) collaborative Protection Profile for Network Devices, v2.2e (CPP_ND_V2.2E)

b) collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625 (MOD_CPP_FW_v1.4e)

c) PP-Module for Virtual Private Network (VPN) Gateways Version 1.2 (MOD_VPNGW_v1.2)

1.3.2 Evaluated Software and Hardware

6 The Target of Evaluation (TOE) is the ID Technologies GoSilent Cube + GoSilent Server v25.01:

a) Build: 25.01.4 (GoSilent Server)

b) Build: 25.01.3 (GoSilent Cube)

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

1.3.3 Evaluated Functions

8 The list of evaluated security functions addressed by this evaluation are included in ST section 2.3.

9 No claims are made regarding any other security functionality.

1.3.4 Functions not included in the TOE Evaluation

10 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.

1.3.5 Non-TOE Components

11 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) **OCSP Server/CDP.** The TOE communicates with an external OCSP Server and CDP for the purposes of certificate checking.

1.3.6 Evaluation Assumptions

12 The following assumptions were made in performing the Common Criteria evaluation as per the CPP_ND_V2.2E, MOD_CPP_FW_v1.4e, and MOD_VPNGW_v1.2. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 1: Evaluation Assumptions (CPP_ND_V2.2e)

Assumption	Guidance
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.

Assumption	Guidance
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.
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 (applies to distributed TOEs only)	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 (applies to vNDs only)	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 (applies to vNDs only)	Ensure all relevant updates pertaining to the security and critical functionality of the TOE are applied in a timely and controlled fashion.
A.VS_ISOLATON (applies to vNDs only)	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 (applies to vNDs only)	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.

Table 2: Evaluation Assumptions (MOD_VPNGW_v1.2)

Assumption	Guidance
A.CONNECTIONS	Ensure network segmentation is employed within the operational environment and that the appropriate TOE interfaces are connected to the appropriate network.

13 No additional assumptions identified in MOD_CPP_FW_v1.4e.

1.4 Conventions

14 The following conventions are used in this guide:

a) **GUI > Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File > Save** to save the file.

b) [REFERENCE] *Section* – denotes a document and section reference from Table 3. For example:

Follow [ADMIN] *Configuring Users* to add a new user.

1.5 Related Documents

15 This guide supplements the below documents which are available from ID Technologies' web portal.

Table 3: Related Documents

Reference	Document
[ST]	ID Technologies GoSilent Cube + GoSilent Server v25.01 Security Target, v1.18 | December 2022

16 **NOTE:** The information in this guide supersedes related information in other documentation.

1.6 Terminology

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

Table 4: Terminology

Term	Definition
CC	Common Criteria
CDP	Certificate Distribution Point

Term	Definition
cPP	Collaborative Protection Profile
CSR	Certificate Signing Request
Cube	ID Technologies GoSilent Cube
GSS	ID Technologies GoSilent Server
GUI	Graphical User Interface
NAT	Network Address Translation
OCSP	Online Certificate Status Protocol
PAT	Port Address Translation
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network

2 Secure Acceptance

2.1 Obtaining the TOE

18 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.

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

2.2 Installation and Verification

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

a) **GoSilent Server**

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

Maintenance > About

b) **GoSilent Cube**

- Log into the Cube GUI as described in section 3.1 and navigate to the following:

Help > About This GoSilent

21 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 an ID Technologies security key. This signature is checked against the ID Technologies 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. ID Technologies should be contacted for support if subsequent failures occur.

22 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.

23 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'.*

24 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.

25 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.

26 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.

27 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

28 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

29 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.

30 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

31 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

32 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.

33 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.

34 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.

35 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.

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

a) ICMPv4 (Type, Code)

b) ICMPv6 (Type, Code)

c) IPv4 (Source address, Destination address, Transport Layer Protocol)

d) IPv6 (Source address, Destination address, Transport Layer Protocol)

e) TCP (Source port, Destination port)

f) UDP (Source port, Destination port)

37 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.

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

a) IPv4 (RFC 791)
   - Source Address
   - Destination Address
   - Protocol

b) IPv6 (RFC 8200)
   - Source Address
   - Destination Address
   - Next Header (Protocol)

c) TCP (RFC 793)
   - Source Port
   - Destination Port

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

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

39 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.

40 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

41 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

42 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.

43 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.

44 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.

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

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

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

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

48 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.

49 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
```

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

51 Additional information on audit logging is described in Section 3.10.

3.3.3 GSS Administrator Access

3.3.3.1 Enable Remote Access

52 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.

53 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 45 and substitute the IP address of the allowed administrator system.
- Navigate to rule 43 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 49.

3.3.3.3 Verify Firewall Configuration

54 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.

55 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

56 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)

57 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

58 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*'.

59 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

60 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.

61 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

62 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.
(Note: this parameter should be configured to at least 8 characters).

63 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.

64 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

65 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.

66 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.

67 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.

68 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 ID Technologies in the event any component fails the power-up tests.

3.8 VPN

3.8.1 IPsec VPN Configuration

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

70 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-pfsha384-ecp384 (Top Secret DH20)

  Can configure to:
  aes128gcm16-prfsha256-ecp256 (Secret DH19)

  aes128-sha1-modp2048 (DH14)

  aes128-sha1-ecp256

  aes128-sha1-ecp384

  aes256-sha256-modp2048

  aes256-sha256-ecp256

  aes256-sha256-ecp384

  aes128gcm16-prfsha256-modp2048

  aes128gcm16-prfsha256-ecp384

  aes256gcm16-prfsha384-modp2048

  aes256gcm16-prfsha384-ecp256

- '*Security Association (SA) Lifetime*' – Between 1 and 24 hours
- '*Child SA Lifetime*' – Between 1 and 8 hours
- '*Enable Strict OCSP Checking*' – Must be enabled

71 As described further in Section 3.9, 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.

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

3.8.2 Virtual Server Configuration

73 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*'.

3.9 Network

74 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.)

75 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.

76 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.

77 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.

78 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

79 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.

80 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.

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

82 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*' – Must be set to '*AES128-GCM-SHA256*' or '*ECDHE-ECDSA-AES256-GCM-SHA384*'.
- '*Reject wildcard TLS server certificates*' – Must be enabled.
- '*Enable CRL checking*' – Must be enabled.

83 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.

84 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.

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

3.11 Cryptographic Functions

86 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 – RSAES-PKCS1-v1_5 and Elliptic-curve (P-384)

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

c) IKE/IPsec - Elliptic-curve (P-256, P-384) and FFC safe-primes (RFC 3526 DH14)

87 The TOE performs cryptographic key generation services during IPsec tunnel establishment for IKE peer authentication using ECDSA P-256 and P-384 Elliptic curve keys as specified in FIPS Pub 186-4 "Digital Signature Standard (DSS)" Appendix B.4 and FFC schemes using safe-prime groups that meet NIST SP 800-56A Revision 3 and per RFC3526 DH14. These keys are used in the Diffie-Hellman process for IPsec and produce key sizes equivalent to or greater than 112 bits. Additional information on the specification of algorithms used for IPsec connections can be found in Section 3.8

88 The TOE performs cryptographic signature generation and verification services using ECDSA P-256 and P-384 in support of IPsec, TLS, X509, and trusted update functions. RSA signature generation and verification services are also used to support TLS client connections. Additional information on certificate parameters can be found in section 3.12

89 The TOE only supports TLSv1.2 when acting as a TLS client to provide a trusted channel to the Syslog server. In this case, the Cube will always initiate the connection using the following ciphersuites:

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

These ciphersuites can be configured as described in sections 3.8 and 3.10.

90 When the TOE acts as a TLS/HTTPS server to provide the administrative web GUI, only TLSv1.2 is supported and uses the following ciphersuite:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

91 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 SHA256 will include HMAC-SHA-256.

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

3.12 Certificate Management

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

94 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.

95 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.

96 The TOE supports ECDSA key pair generation using P-256 and P-384 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.

97 The TOE supports ECDSA key establishment using P-256 and P-384 curves.

98 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 "IKEv2" or "WebDashboard" are provided for the administrator to define the certificate usage.

99 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-256 or P-384 can be selected from the drop-down menu.

On GSS, navigate to the following:

'Maintenance > Certificates > Create CSR'

Key size P-256 or P-384 can be selected from the drop-down menu.

100 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.

101 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

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

103 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.

4 Annex A: Log Reference

4.1 Format

104 Each audit record includes the following fields:

a) Date/Timestamp

b) Event Type

c) Subject Identity

d) Event Outcome (Success/Failure)

4.2 Events

105 The TOE generates the following log events:

Table 5: Audit Events

Requirement	Auditable Event	Additional Audit Record Contents	Log
FCO_CPC_ EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoint pairs enabled or disabled.	GoSilent Server: "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 11[IKE] authentication of 'CN=<ip_address>' with ECDSA_WITH_SHA384_DER successful", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 11[IKE] authentication of 'CN=<ip_address>' (myself) with ECDSA_WITH_SHA384_DER successful", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 11[IKE] IKE_SA 10-222-5-144[3] established between <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address>]", GoSilent Cube: "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[IKE] received end entity cert \"CN=<ip_address>, CN=<ip_address>\"",

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] looking for peer configs matching <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address>, CN=<ip_address>]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] no matching peer config found",
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure	GoSilent Server: "<DATE_YYYY-MM-DD><TIME_HH:MM:SS>- [info] 1685#1685: *1010 SSL_do_handshake() failed (SSL: error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol) while SSL handshaking, client: <ip_address>, server: <ip_address>:443", GoSilent Cube: <DATE_YYYY-MM-DD><TIME_HH:MM:SS>- [info] 2044#2044: *69 SSL_do_handshake() failed (SSL: error:1408A0C1:SSL routines ssl3_get_client_hello:no shared cipher) while SSL handshaking, client: <ip_address>, server: <ip_address>:443
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.	GoSilent Server: "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[IKE] received end entity cert \"CN=<ip_address>?\"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] looking for peer configs matching <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address>?]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] no matching peer config found", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[IKE] peer supports MOBIKE", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[ENC] generating IKE_AUTH response 1 [N(AUTH_FAILED)]", GoSilent Cube:

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[ENC] parsed IKE_AUTH response 1 [N(AUTH_FAILED)]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[IKE] received AUTHENTICATION_FAILED notify error"
FCS_TLSC_ EXT.1	Failure to establish a TLS Session	Reason for failure	GoSilent Server: "<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[1953]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure', location='/etc/syslog-ng/syslog-ng.conf:270:5'", GoSilent Cube: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to verify a server certificate from <ip_address>:<port> (Status code (4114) :: The certificate does not contain the Server Auth in the Extended Key Usage field) client_framework 1 /home/admin/client_framework/common/logging/log_shipping/shipping.py 601 gosilent.client_framework.app logger",
FCS_TLSS_ EXT.1	Failure to establish a TLS Session	Reason for failure	GoSilent Server: "<DATE_YYYY/MM/DD> <TIME_HH:MM:SS> [info] 1685#1685: *1010 SSL_do_handshake() failed (SSL: error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol) while SSL handshaking, client: <ip_address>, server: <ip_address>:443", GoSilent Cube:

Requirement	Auditable Event	Additional Audit Record Contents	Log
			<DATE_YYYY/MM/DD> <TIME_HH:MM:SS> [info] 2044#2044: *69 SSL_do_handshake() failed (SSL: error:1408A0C1:SSL routines: ssl3_get_client_hello: no shared cipher) while SSL handshaking, client <ip_address>, server <ip_address>:443
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation.	Source and destination address Source and destination ports Transport Layer Protocol TOE Interface	"<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise kernel: [firewall_custom_log] ACCEPT IN=eth0 OUT=eth1 MAC=<mac_address> SRC=<ip_address> DST=<ip_address> LEN=20 TOS=0x00 PREC=0x00 TTL=63 ID=1 PROTO=87", "<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise kernel: [firewall_custom_log] ACCEPT IN=eth0 OUT=eth1 MAC=<mac_address> SRC=<ip_address> DST=<ip_address> LEN=20 TOS=0x00 PREC=0x00 TTL=63 ID=1 PROTO=88",
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Attempting to login from origin ip (<ip_address>) and username (<username>) core_server 1 ./app/console_user/console_user_api.py 37 gosilent.core_server.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> 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 ./app/console_user/console_user_api.py 107 gosilent.core_server.app logger", GoSilent Cube: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to login (IP: <ip_address>, username: <username>): attempts: 1 client_framework 1 /home/<username>/client_framework/app/console_user.py 97 gosilent.client_framework.app logger"

Requirement	Auditable Event	Additional Audit Record Contents	Log
FIA_UIA_ EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Attempting to login from origin ip (<ip_address>) core_server 1 ./app/console_user/console_user_api.py 29 gosilent.core_server.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to login, origin ip (<ip_address>) and username (<username>), (4084) Could not login console user core_server 0 ./app/console_user/console_user_api.py 120 gosilent.core_server.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not login origin ip (<ip_address>), (4081) Too many failed login attempts. Please try again later. core_server 0 ./app/console_user/console_user_api.py 45 gosilent.core_server.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Successfully logged in from origin ip (<ip_address>) (id:6, username:<username>) 1 ./app/console_user/console_user_api.py 106 gosilent.core_server.app logger", GoSilent Cube: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO ***** Login attempted ***** client_framework 1 /home/<username>/client_framework/app/<user>.py 67 gosilent.client_framework.app logger", “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to login (IP: <ip_address>, username: <username>): attempts: 1 client_framework 1 /home/<username>/client_framework/app/console_user.py 97 gosilent.client_framework.app logger” "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Logged in successfully (IP: <ip_address>) client_framework 1 /home/<username>/client_framework/app/<user>.py 99 gosilent.client_framework.app logger",

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Attempting to login from origin ip (<ip_address>) core_server 1 ./app/console_user/console_user_api.py 32 gosilent.core_server.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Successfully logged in from origin ip (<ip_address>) (id:6, username:<username>) 1
FIA_UAU_ EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to login, origin ip (<ip_address>) and username (<username>), (4084) Could not login console user core_server 0 ./app/console_user/console_user_api.py 120 gosilent.core_server.app logger", GoSilent Cube: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO ***** Login attempted ***** client_framework 1 /home/<username>/client_framework/app/<user>.py 67 gosilent.client_framework.app logger", “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to login (IP: <ip_address>, username: <username>) attempts: 1 client_framework 1 /home/<username>/client_framework/app/console_user.py 97 gosilent.client_framework.app logger” "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Logged in successfully (IP: <ip_address>) client_framework 1 /home/<username>/client_framework/app/<user>.py 99 gosilent.client_framework.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Attempting to login from origin ip (<ip_address>) core_server 1 ./app/console_user/console_user_api.py 32 gosilent.core_server.app logger",

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Successfully logged in from origin ip (<ip_address>) (id:6, username:<username>) 1
FIA_X509_ EXT.1/ITT	Unsuccessful attempt to validate a certificate. Any addition, replacement, or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation. Identification of certificates added, replaced, or removed as trust anchor in the TOE's trust store.	GoSilent Server: **Failure-** " DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[ENC] parsed IKE_AUTH response 1 [IDr CERT AUTH CPRP(ADDR DNS DNS) SA TSi TSr]", "2019-08-06T13:20:03+0000 13[IKE] received end entity cert \"CN=<ip_address>\"", " DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] using certificate \"CN=<ip_address>\"", " DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-+0000 13[CFG] using trusted intermediate ca certificate \"C=<C>, O=<O>, OU=<OU>, CN=<CN>"", " DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-+0000 13[CFG] subject certificate invalid (valid from <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY> to <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY>)", " DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[IKE] no trusted ECDSA public key found for 'CN=<ip_address>'" "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 10[CFG] selected peer config '<ip_address>' using certificate "CN=<ip_address>" using trusted intermediate ca certificate "CN=<ipsec_ca>" subject certificate invalid (valid from <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY> to <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY>) **Trust store-** "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not import certificates (<certificate_identifier>) - Unnamed curves are not supported for EC public keys - explicit curve parameters are not allowed. (id:6, username:<username>) 1

Requirement	Auditable Event	Additional Audit Record Contents	Log
			./app/certificate_management/certificate_management_api.py 870 gosilent.core_server.app logger", GoSilent Cube: **Failure-** “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[CFG] using certificate “CN=<ip_address>” using trusted intermediate ca certificate “CN=<ipsec_ca>” subject certificate invalid (valid from <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY> to <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY>) "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[CFG] no issuer certificate found for \"CN=<ip_address>\"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[CFG] issuer is \"C=<C>, O=<O>, OU=<OU>, CN=<CN>"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[IKE] no trusted ECDSA public key found for 'CN=<ip_address>'", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[ENC] generating INFORMATIONAL request 2 [N(AUTH_FAILED)]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] subject certificate invalid (valid from <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY> to <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY>)", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[IKE] no trusted ECDSA public key found for 'CN=<ip_address>'", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 15[CFG] certificate was revoked on <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY> reason: unspecified", **Trust store-** "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not retrieve the local issuer CA object of the server certificate from <ip_address>:<port> (Status code (4031) :: CA chain was not found.) client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 651 gosilent.client_framework.app logger",

Requirement	Auditable Event	Additional Audit Record Contents	Log
FIA_X509_ EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure. Identification of certificates added, replaced, or removed as trust anchor in the TOE's trust store.	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not retrieve the local issuer CA object of the server certificate from <ip_address>:<port> (Status code (4031) :: CA chain was not found.) <vpn_server> 1 ./common/logging/log_shipping/shipping.py 651 gosilent.vpn_server.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not get server certificate from <ip_address>:<port> (The certificate does not contain the Server Auth in the Extended Key Usage field) vpn_server 1 ./common/logging/log_shipping/shipping.py 284 gosilent.vpn_server.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[1333]: Syslog connection failed; fd='22', server='AF_INET(<ip_address>:<port>)', error='Connection refused (111)', time_reopen='300'", "<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[1333]: Certificate valid, but purpose is invalid; location='/etc/syslog-ng/syslog-ng.conf:251:5'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[1333]: Certificate subject does not match configured hostname; hostname='<ip_address>', certificate='<ip_address>'", "<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[1333]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed', location='/etc/syslog-ng/syslogng.conf:251:5'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[15090]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed', location='/etc/syslog-ng/syslogng.conf:259:5'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[28117]: Certificate validation failed; subject='CN=<ip_address>, OU=<OU>, O=<O>, C=<C>', issuer='CN=<CN>, OU=<OU>, O=<O>, C=<C>', error='certificate has expired', depth='0'",

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not get server certificate from <ip_address>:<port> client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 264 gosilent.client_framework.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not enable the log shipping (could not download/save CRL). Disabling... client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 412 gosilent.client_framework.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not found any CRLs from the download server cert (<cert_id>) client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 336 gosilent.client_framework.app logger", GoSilent Cube: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not retrieve the local issuer CA object of the server certificate from <ip_address>:<port> (Status code (4031) :: CA chain was not found.) client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 651 gosilent.client_framework.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to verify the certificate: The certificate does not contain the Server Auth in the Extended Key Usage field client_framework 1 /home/<username>/client_framework/common/certificate/certs.py 1406 gosilent.client_framework.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not get server certificate from <ip_address>:<port> (The certificate does not contain the Server Auth in the Extended Key Usage field) client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 284 gosilent.client_framework.app logger", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[26047]: SSL error while writing stream; tls_error='SSL

Requirement	Auditable Event	Additional Audit Record Contents	Log
			routines:ssl3_get_server_hello:wrong cipher returned', location='/etc/syslog-ng/syslog-ng.conf:258:5'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[26047]: I/O error occurred while writing; fd='24', error='Broken pipe (32)'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[12137]: Certificate subject does not match configured hostname; hostname='<ip_address>', certificate='<ip_address>'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[12137]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed', location='/etc/syslog-ng/syslog-ng.conf:258:5'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[12137]: I/O error occurred while writing; fd='24', error='Broken pipe (32)'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[12137]: Syslog connection broken; fd='24', server='AF_INET(<ip_address>:<port>)', time_reopen='300'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[15090]: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed', location='/etc/syslog-ng/syslog-ng.conf:259:5'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[15090]: Syslog connection broken; fd='18', server='AF_INET(<ip_address>:<port>)', time_reopen='300'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[28117]: Certificate validation failed; subject='CN=<CN>, OU=<OU>, O=<O>, C=<C>', issuer='CN=<CN>, OU=<OU>, O=<O>, C=<C>', error='certificate has expired', depth='0'", "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Could not get server certificate from <ip_address>:<port> client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 264 gosilent.client_framework.app logger",

Requirement	Auditable Event	Additional Audit Record Contents	Log
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Retrieved OTA bundle index (id:6, username:<username>) 1 ./app/enterprise/enterprise_client_ota_management.py 166 gosilent.core_server.app logger", GoSilent Cube: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO downloading new swu (id:1, username:<username>) 1 /home/<username>/client_framework/app/scripts/ota_controller.py 195 gosilent.client_framework.app logger",
FMT_MOF.1/ Services	Ability to start and stop services	None.	GoSilent Server: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (logging.shipping.enabled) with value of (False)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (logging.shipping.enabled) with value of (True)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully connected to a server profile ({'vpn_connection_timeout': 30000, 'profile_id': 5, 'server_name': u'<ip_address>'})", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/scripts/connection_management/connection_manager.py", "line": 725, "logger": "gosilent.client_framework.app logger"}

Requirement	Auditable Event	Additional Audit Record Contents	Log
			{"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Disconnecting from a server profile ({'profile_id': 5, 'server_name': u'<ip_address>'})", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/scripts/connection_management/connection_manager.py", "line": 295, "logger": "gosilent.client_framework.app logger"}
FMT_SMF.1	All management activities of TSF data.	None.	Ability to administer the TOE locally and remotely: • FTA_SSL.3 • FTA_SSL_EXT.1 • FTA_SSL.4 Ability to update the TOE and to verify the updates: • FPT_TUD_EXT.1 Ability to start and stop services • FMT_MOF.1/Services Ability to manage the cryptographic keys: • FIA_X509_EXT.1/ITT Ability to configure the interaction between TOE components: • FCO_CPC_EXT.1 • FPT_ITT.1 Ability to set the time which is used for timestamps: • FPT_STM_EXT.1 Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors: • FIA_X509_EXT.1/ITT Ability to import X509v3 certificates to the trust store: • FIA_X509_EXT.1/ITT

Requirement	Auditable Event	Additional Audit Record Contents	Log
			Ability to configure the access banner: GoSilent Server: "[pid: <PID>|app: 0|req: 1960/1960] <ip_address> () {<number> vars in <number> bytes} [<DATE_TIME>] GET /api/v1/settings/admin_console.login.banner.enabled => generated <number> bytes in 2 msecs (HTTP/1.1 200) <number> headers in <number> bytes (3 switches on core 98)", {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (admin_console.login.banner.text) with value of (TEST BANNER GSS)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO System Setting (client.login.banner.enabled) has changed, updating to (True) (id:1, username:<username>) 1 /home/<username>/client_framework/app/system_settings/system_settings.py 168 gosilent.client_framework.app logger" {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "System setting (client.login.banner.text) has changed, updating to (TEST BANNER CUBE)", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/system_settings/system_settings.py", "line": 168, "logger": "gosilent.client_framework.app logger"} Ability to configure the session inactivity time: GoSilent Server:

Requirement	Auditable Event	Additional Audit Record Contents	Log
			{"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (admin_console.session.inactivity.interval) with value of (30)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "System setting (client.session.inactivity.interval) has changed, updating to (60)", "user" : "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/system_settings/system_settings.py", "line": 168, "logger": " gosilent.client_framework.app logger"} Ability to configure authentication failure parameters: GoSilent Server: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (admin_console.login.lockout.attempts) with value of (5)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "System setting (client.login.lockout.attempts) has changed, updating to (5)", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/system_settings/system_settings.py", "line": 168, "logger": "gosilent.client_framework.app logger"}

Requirement	Auditable Event	Additional Audit Record Contents	Log
			Ability to modify the behavior of the transmission of audit data to an external IT entity: GoSilent Server: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (logging.shipping.enabled) with value of (True)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Log shipping is being updated: ENABLE_SHIPPING", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/common/logging/log_shipping/shipping.py", "line": 92, "logger": "gosilent.client_framework.app logger"} Ability to configure the cryptographic functionality: GoSilent Server: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (logging.shipping.tls.cipher.id) with value of (2)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (vpn.ipsec.cipher.suite) with value of (2)", "user": "(id:6, username:<username>)", "userid": "1", "file":

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "System setting (logging.shipping.tls.cipher) has changed, updating to (AES128-GCM-SHA256)", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/system_settings/system_settings.py", "line": 168, "logger": "gosilent.client_framework.app logger"} Ability to configure the lifetime for IPSec SAs: GoSilent Server: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (vpn.sa.lifetime.strongswan) with value of (1200)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (vpn.child.sa.lifetime.strongswan) with value of (300)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "System setting (vpn.child.sa.lifetime.strongswan) has changed, updating to (300)", "user": "(id:1, username:<username>)", "userid": "1", "file":

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"/home/<username>/client_framework/app/system_settings/system_settings.py", "line": 168, "logger": "gosilent.client_framework.app logger"} {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Updated SA lifetime for {'profile_id': 5, 'server_name': u'<ip_address>'}: IKE Nonem, CHILD Nonem", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/models/vpn_profile/vpn_profile_controller.py", "line": 665, "logger": "gosilent.client_framework.app logger"} Ability to configure the reference identifier for the peer: GoSilent Server: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "Successfully updated default system setting with key (<key_url>) with value of (<value_url>)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ", "type": "INFO", "msg": "System setting (logging.destination.url) has changed, updating to (<url>)", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/system_settings/system_settings.py", "line": 168, "logger": "gosilent.client_framework.app logger"}
FMT_SMF.1/ FFW	All management activities of TSF data (including creation, modification,	None.	The following audit logs are generated when firewall rules are created, modified, or deleted and the firewall profile is saved to the TOE: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Successfully retrieved firewall profile (<profile>) for the interface (all) (id:6, username:<username>) 1 ./common/firewall/firewall.py 263 gosilent.core_server.firewall log",

Requirement	Auditable Event	Additional Audit Record Contents	Log
	and deletion of firewall rules).		"<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Got the advanced firewall rules for ipv4 (number of lines: 645) (id:6, username:<username>) 1 ./app/firewall/firewall_api.py 233 gosilent.core_server.firewall log",
FMT_SMF.1/ VPN	All administrative actions	No additional information.	GoSilent Server: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS>", "type": "INFO", "msg": "Successfully updated default system setting with key (vpn.sa.lifetime.strongswan) with value of (1800)", "user": "(id:6, username:<username>)", "userid": "1", "file": "./models/system_setting/system_setting_controller.py", "line": 198, "logger": "gosilent.core_server.app logger"} GoSilent Cube: {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS>", "type": "INFO", "msg": "System setting (vpn.child.sa.lifetime.strongswan) has changed, updating to (600)", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/system_settings/system_settings.py", "line": 168, "logger": "gosilent.client_framework.app logger"}
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport layer protocol	"<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise kernel: [firewall_custom_log] ACCEPT IN=eth0 OUT=eth1 MAC=<mac_address> SRC=<ip_address> DST=<ip_address> LEN=20 TOS=0x00 PREC=0x00 TTL=63 ID=1 PROTO=87", "<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise kernel: [firewall_custom_log] ACCEPT IN=eth0 OUT=eth1 MAC=<mac_address> SRC=<ip_address> DST=<ip_address> LEN=20 TOS=0x00 PREC=0x00 TTL=63 ID=1 PROTO=88",

Requirement	Auditable Event	Additional Audit Record Contents	Log
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	GoSilent Server: **Initiation-** “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 11[IKE] authentication of ‘CN=<ip_address>’ with ECDSA_WITH_SHA384_DER successful”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 11[IKE] authentication of ‘CN=<ip_address>’ (myself) with ECDSA_WITH_SHA384_DER successful”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 11[IKE] IKE_SA <sa>[3] established between <ip_address>[CN=<ip_address>]…<ip_address>[CN=<ip_address”>]", DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-<ip_address“ {"vpn_username“: "<ip_address","status_type":"Connected","program":"vpnevent-monitor","origin_ip":"<ip_address”","ike_state":"ESTABLISHED","host":"<host_id","event_type":"child-updown","event_date":"DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-+00:00","child_state":"INSTALLED","bytes_out”:”0","bytes_in”:”0"} " DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-+0000 12[IKE] IKE_SA <sa>[142] established between <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address”>]", **Termination-** "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 15[ENC] parsed INFORMATIONAL request 2 [”]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 15[IKE] received DELETE for IKE_SA <sa>”1]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 15[IKE] deleting IKE_SA <sa>[1] between <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address”>]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 15[IKE] IKE_SA deleted", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0500 15[ENC] generating INFORMATIONAL response 2 ”]"“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 16[ENC] parsed INFORMATIONAL response 2 ”]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[CFG] vici terminate IKE_SA '8b1c7bec-d3db-11e9-83d70201bbf30606"',

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[IKE] deleting IKE_SA 8b1c7bec-d3db-11e9-83d7-0201bbf30606[40] between <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address”>]", **Failure-** "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[IKE] received end entity cert \"CN=<ip_address”\"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] looking for peer configs matching <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address”]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] no matching peer config found", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[ENC] generating IKE_AUTH response 1 [N(AUTH_FAILED)]",“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[ENC] parsed INFORMATIONAL_V1 request 226795256 [N(NO_PROP)]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[IKE] received NO_PROPOSAL_CHOSEN error notify", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[CFG] vici terminate IKE_SA '1671fca2-cb22-11e9-a88d0201bbf30’”6'",“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] no acceptable ENCRYPTION_ALGORITHM found", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_”EQ", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] configured proposals: ESP:AES_CBC_128/HMAC_SHA1_96/MODP_2048/NO_EXT_”EQ", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[IKE] no acceptable proposal found",“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[ENC] parsed IKE_AUTH response 1 [IDr CERT AUTH CPRP(ADDR DNS DNS) Sa TSi TSr]", “ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[IKE] received end entity cert \"CN=<ip_address”\"",

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] using certificate \"CN=<ip_address”\"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] using trusted intermediate ca certificate \"C=<C>, O=<O>, OU=<OU>, CN=<CN>\"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] subject certificate invalid (valid from <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY> to <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYY”>)", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[IKE] no trusted ECDSA public key found for 'CN=<ip_address”>"' GoSilent Cube: **Initiation-** “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] authentication of ‘CN=<ip_address>’ with ECDSA_WITH_SHA384_DER successful” “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] <sa> profile-5-cn[226] established between <ip_address>[CN=<ip_address>] … <ip_address>[CN=<ip_address>]”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] scheduling rekeying in 14326s”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] maximum IKE_SA lifetime 15766s”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] installing DNS server <ip_address> via resolvconf”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] installing new virtual IP <ip_address>”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[CFG] selected proposal: ESP:AES_CBC_12/HMAC_SHA1_96/NO_EXT_SEQ”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] CHILD_SA profile-5-cn{208} established with SPIs <spi> and TS <ip_address> ““ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[NET] received packet: from <ip_address>[500] to <ip_address>[500] (36 bytes)"“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[ENC] parsed IKE_SA_INIT response 0 [N(NO_PROP)]"“

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[IKE] received NO_PROPOSAL_CHOSEN notify error“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[CFG] vici terminate IKE_SA 'e955f3c4-d30d-11e9-83d7-0201bbf30’”6'", “ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[CFG] loaded ANY private key“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[CFG] vici initiate CHILD_SA 'e955f3c4-d30d-11e9-83d7-0201bbf30’”6'",“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 11[CFG] vici initiate CHILD_SA 'e955f3c4-d30d-11e9-83d7-0201bbf30’”6'", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 15[IKE] initiating IKE_SA e955f3c4-d30d-11e9-83d7-0201bbf30606[36] to <ip_address>", “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS> INFO Successfully connected to a server profile ({‘vpn_connection_timeout’: 300000, ‘profile_id’: u’4ebd4c42-a255-11e9-87b1-0050b622ccf2’, ‘server_name’: ‘,<ip_address>’}) (id:1, username:<username>) 1 /home/<username>/client_framework/common/vici/client/client_connection_functions.py 687 gosilent.client_framework.app logger” **Termination-** “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 12[CFG] vici terminate IKE_SA ‘profile-5-cn’ “, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 14[IKE] deleting IKE_SA profile-5-cn[226] between <ip_address>[CN=<ip_address>] … <ip_address>[CN=<ip_address>]”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 14[IKE] sending DELETE for IKE_SA profile-5-cn[226]”, “<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 14[ENC] generating INFORMATIONAL request 2 [D]”,

Requirement	Auditable Event	Additional Audit Record Contents	Log
			Failure- "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[NET] received packet: from <ip_address>[<port>] to <ip_address>[<port>] (76 bytes)", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[ENC] parsed IKE_AUTH response 1 [N(AUTH_FAILED]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[IKE] received AUTHENTICATION_FAILED notify error" "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[CFG] vici terminate IKE_SA 'e955f3c4-d30d-11e9-83d7-0201bbf30'"6"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] selecting proposal:", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] no acceptable ENCRYPTION_ALGORITHM found", " "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_"EQ", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] configured proposals: ESP:AES_CBC_128/HMAC_SHA1_96/MODP_2048/NO_EXT_"EQ", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[IKE] no acceptable proposal found" "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[IKE] no trusted ECDSA public key found for 'CN=<ip_address>', "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 10[ENC] generating INFORMATIONAL request 2 [N(AUTH_FAILED"]"" "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS> ERROR Failed to connect to a server profile'({'vpn_connection_timeout': 300000' 'profile_id'' u'f9bde8ae-c4b0-11e9-870a-0201efc3e'60', 'server_name: '<ip_address>'}): Invalid credentials could not connect to profile (id:1, username:<username>) 1 /home/<username>/client_framework/common/vici/client/client_connection_functions.py 703 gosilent.client_framework.app logger",

Requirement	Auditable Event	Additional Audit Record Contents	Log
FPT_TUD_ EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	GoSilent Server: “ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Retrieved OTA bundle index (id:6, username:<username>) 1 ./app/enterprise/enterprise_client_ota_management.py 166 gosilent.core_server.app logger",“ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR 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' (id:6, username:<username>) 1 ./common/crypto/sign_verify.py 138 gosilent.core_server.app logger“ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Service pack has an invalid signature, overlay signature “ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> WARNING An error has occurred while trying to unarchive the service pack. (7702) Provided archive bundle cannot be decompressed (id:6, username:<username>) 1 ./app/enterprise/enterprise_servicepack_utils.py 85 gosilent.core_server.app logger", GoSilent Cube: “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO OTA update was performed successfully. Restoring settings. ota 1 /home/-<username>/client_framework/first_boot_after_update_runner.py 130 gosilent.ota.pre_scripts_log” <DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO checking checksum of OTA swu file (id:6, username: <username>) 1 . <DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to import the OTA bundle: Checksum check failed for OTA swu file

Requirement	Auditable Event	Additional Audit Record Contents	Log
FPT_STM_ EXT.1	Discontinuous changes to ti–e - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT. 1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Setting system date and time to '<DATE_YYYY-MM-DD>T<TIME_HH:MM>'(id:6, username:<username>) 1 ./common/system/system_management.py 153 gosilent.core_server.system log", GoSilent Cube: “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO System setting (network.set.time.manually) has changed, updating to (True) (id: 1, username: <username>) 1 /home/<username>/client_framework/app/system_settings/system_settings.py 168 gosilent.client_framework.app logger”“ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Successfully set the system date and time (id:1, username:<username>) 1 /home/<username>/client_framework/common/system/system_management.py 144 gosilent.client_framework.system log"
FTA_SSL_ EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO User (7) was auto logged out, (id:7, username:<username>) 1 ./app/console_user/console_user_api.py 172 gosilent.core_server.app logger", GoSilent Cube: “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Logged out automatically because of inactivity (username: <username>) (id:6, username:<username>) 1 /home/<username>/client_framework/app/core_app.py 117 gosilent.client_framework.app logger”, “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Getting system settings client_framework 1

Requirement	Auditable Event	Additional Audit Record Contents	Log
			/home/<username>/client_framework/app/system_settings/system_settings.py 56 gosilent.client_framework.app logger”,
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	GoSilent Server: “ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO User (7) was auto logged out, origin ip (<ip_address>) (id:7, username:<username>) 1 ./app/console_user/console_user_api.py 172 gosilent.core_server.app logger", GoSilent Cube: “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Logged out automatically because of inactivity (IP: <ip_address>, username: <username>) (id:1, username:<username>) 1 /home/<username>/client_framework/app/core_app.py 117 gosilent.client_framework.app logger”,
FTA_SSL.4	The termination of an interactive session.	None.	GoSilent Server: "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO User (6) is logging out, origin ip (<ip_address>) (id:6, username:<username>) 1 ./app/console_user/console_user_api.py 146 gosilent.core_server.app logger", GoSilent Cube: “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Logged out successfully (IP: <ip_address>, username: <username>) (id:1, username:<username>) 1 /home/<username>/client_framework/app/core_app.py 117 gosilent.client_framework.app logger”,

Requirement	Auditable Event	Additional Audit Record Contents	Log
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	GoSilent Server: **Initiation-** "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Enabling log shipping... vpn_server 1 ./common/logging/log_shipping/shipping.py 137 gosilent.vpn_server.app logger"“ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[1333]: Syslog connection established; ’d=’22', server='AF_INET(<ip_address>:<port>', local='AF_INET(<ip_address>’”)"", **Termination-** "<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[3039]: Syslog connection broken; ’d=’15', server='AF_INET(<ip_address>:<port>)', time_reopen='300"“ **Failure-** "<DATE_MMM DD> <TIME_HH:MM:SS> silent-edge-enterprise syslog-ng[1953]: SSL error while writing stream; tls_error='SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure', location='/etc/syslog-ng/syslog-ng.conf:270:5"“, GoSilent Cube: **Initiation-** “ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Enabling log shipping... (id:1, username:<username>) 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 137 gosilent.client_framework.app logger",“ "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> gosilent syslog-ng[12137]: Syslog connection established; ’d=’24', server='AF_INET(<ip_address>:<port>)', local='AF_INET(<ip_address>’”)"", **Termination-**

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_MMM DD> <TIME_HH:MM:SS> gosilent syslog-ng[18955]: Syslog connection broken; 'd='22', server='AF_INET(<ip_address>:<port>)', time_reopen='300'" **Failure-**" "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> ERROR Failed to verify a server certificate from <ip_address>:<port> (Status code (4114) :: The certificate does not contain the Server Auth in the Extended Key Usage field) client_framework 1 /home/<username>/client_framework/common/logging/log_shipping/shipping.py 601 gosilent.client_framework.app logger"""
FTP_ITC.1/VPN	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	No additional information. No additional information. Identification of the initiator and target of failed trusted channel establishment attempt.	GoSilent Server: **Initiation-** {"event_type": "child-updown", "bytes_out": 0, "origin_ip": "<ip_address>", "ike_state": "ESTABLISHED", "bytes_in": 0, "vpn_username": "<username>", "client_ipsec_ip_address": "<ip_address>", "event_date": "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+00:00", "vpn_server_uuid": "<uuid>", "status_type": "Connected", "child_state": "INSTALLED"} **Termination-** {"event_type": "child-updown", "bytes_out": 4316, "origin_ip": "<ip_address>", "ike_state": "DELETING", "bytes_in": 1429, "vpn_username": "<username>", "client_ipsec_ip_address": "<ip_address>", "event_date": "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+00:00", "vpn_server_uuid": "<uuid> "status_type": "Disconnected", "child_state": "INSTALLED"} **Failure-** "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[IKE] received end entity cert" \"CN=<ip_address""\"",

Requirement	Auditable Event	Additional Audit Record Contents	Log
			"<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] looking for peer configs matching <ip_address>[CN=<ip_address>]...<ip_address>[CN=<ip_address>]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[CFG] no matching peer config found", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 11[ENC] generating IKE_AUTH response 1 [N(AUTH_FAILED)]",“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[ENC] parsed INFORMATIONAL_V1 request 226795256 [N(NO_PROP)]", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[IKE] received NO_PROPOSAL_CHOSEN error notify", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 09[CFG] vici terminate IKE_SA '1671fca2-cb22-11e9-a88d0201bbf30’”6"',“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] no acceptable ENCRYPTION_ALGORITHM found", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_”EQ", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[CFG] configured proposals: ESP:AES_CBC_128/HMAC_SHA1_96/MODP_2048/NO_EXT_”EQ", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>-0400 09[IKE] no acceptable proposal found",“ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[ENC] parsed IKE_AUTH response 1 [ID CERT AUTH CPRP(ADDR DNS DNS) Sa TSi TS”]", “ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[IKE] received end entity cert” \"CN=<ip_address>\"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] using certificate” \"CN=<ip_address>\"", “ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] using trusted intermediate ca certificate” \"C=<C>, O=<O>, OU=<OU>, CN=<CN>"", "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[CFG] subject certificate invalid (valid from <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYYY> to <DATE_MMM DD> <TIME_HH:MM:SS> <YEAR_YYY”>)", “ "<DATE_YYYY-MM-DD>T<TIME_HH:MM:SS>+0000 13[IKE] no trusted ECDSA public key found for 'CN=<ip_address>"'

Requirement	Auditable Event	Additional Audit Record Contents	Log
			GoSilent Cube: **Initiation-** {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS>", "type": "INFO", "msg": "Trying to connect with a VPN connection identifier (profile-5-cn)", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/scripts/connection_management/connection_manager.py", "line": 886, "logger": "gosilent.client_framework.app logger"} **Termination-** {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS>", "type": "INFO", "msg": "Disconnecting from a server profile ({'profile_id': 5, 'server_name': u'<ip_address>'})", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/scripts/connection_management/connection_manager.py", "line": 295, "logger": "gosilent.client_framework.app logger"} **Failure-** {"timestamp": "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS>", "type": "ERROR", "msg": "Failed to connect to a server profile ({'vpn_connection_timeout': 45000, 'profile_id': 6, 'server_name': u'<ip_address>'}): No internet connection found", "user": "(id:1, username:<username>)", "userid": "1", "file": "/home/<username>/client_framework/app/scripts/connection_management/connection_manager.py", "line": 706, "logger": "gosilent.client_framework.app logger"}
FTP_TRP.1/ Admin	Initiation of the trusted path. Termination of the trusted path.	None.	GoSilent Server: **Initiation-**

Requirement	Auditable Event	Additional Audit Record Contents	Log
	Failure of the trusted path functions.		"<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Attempting to login from origin ip (<ip_address>) and username (<username>) core_server 1 ./app/console_user/console_user_api.py 37 gosilent.core_server.app logger", **Termination-** "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO User (7) was auto logged out, origin ip (<ip_address>) (id:7, username:<username>) 1 ./app/console_user/console_user_api.py 172 gosilent.core_server.app logger", **Failure-** "<DATE_YYYY/MM/DD> <TIME_HH:MM:SS> [info] 1685#1685: *1010 SSL_do_handshake() failed (SSL: error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol) while SSL handshaking, client: <ip_address>, server: <ip_address>:443", GoSilent Cube: **Initiation-** "<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Attempting to login from origin ip (<ip_address>) and username (<username>) core_server 1 ./app/console_user/console_user_api.py 37 gosilent.core_server.app logger", **Termination-** “<DATE_YYYY-MM-DD> <TIME_HH:MM:SS> INFO Logged out automatically because of inactivity (IP: <ip_address>, username: <username>) (id:1, username:<username>) 1 /home/<username>/client_framework/app/core_app.py 117 gosilent.client_framework.app logger”, **Failure-**

Requirement	Auditable Event	Additional Audit Record Contents	Log
			“<DATE_YYYY/MM/DD> <TIME_HH:MM:SS> [info] 2044#2044: *69 SSL_do_handshake() failed (SSL: error:1408A01:SSL routines:ssl3_get_client_hello:no shared cipher) while SSL handshaking, client <ip_address>, server: <ip_address>:443