Common Criteria Administrator Guide

Cellcrypt Server

Ref:	AG-FED-SRV-1
Ver:	0.8.10
Date:	March 31, 2022

Contents

Figures

Tables

Releases

Issue	Description
0.1.0	Initial release
0.1.1	Cosmetic changes
0.2.0	Major overhaul. Removed installation info (now handled in a separate guide)
0.2.1	Updates to audit Stunnel config, Fig.2 and Table 2
0.2.2	Updated Password and Access Restriction section. Added NTP authentication info
0.3.0	Added Stack install Appendix. Appended temp Notes section with info from the SD's
0.4.0	Added appendix for Remote ESC configuration
0.4.1	Updated EMP banner config and login timeout
0.5.0	Updated Certificates and Domains and cosmetic updates
0.6.0	Added Self-Test section and AIDE updates
0.6.1	Removed AIDE config section and added more info in Appendix A
0.6.2	Added SSH signature algorithm. Updated TOE version reference
0.6.3	Changed TOE name and version
0.6.4	Updated Start-up Tests and minor cosmetic changes
0.7.0	Updated text box formats and moved Passwords and Self-test sections up.
0.7.1	Updated to cover guidance requirements in NDcPP SD and MOD_ESC SD
0.8.0	Removed detailed configuration into and replaced with references to other guides
0.8.1	Updated with feedback from evaluator
0.8.2	Updated variables in audit configs, added CDR log example and removed SELinux info
0.8.3	Updated with feedback from evaluator
0.8.4	Updated with feedback from evaluator
0.8.5	Updated restart instructions for services and other changes based on evaluator feedback
0.8.6	Added more info on keys and other changes based on evaluator feedback
0.8.7	Added info on delayed key deletion and addressed other evaluator comments
0.8.8	Point to Installation guide in Introduction
0.8.9	Fixed a minor formatting error after 4.3.2
0.8.10	Updated TOE version

1. INTRODUCTION

This Administrator Guidance is applicable to the Cellcrypt Server Target of Evaluation (TOE). This guide provides the TOE administrator with the necessary instructions to configure the TOE. Installation and maintenance guides are provided separately [Ref 3][Ref 4]. This guide assumes the reader has a working knowledge of networking infrastructure and is familiar with the basic concepts and terminologies used in this environment. It also assumes a working knowledge of Linux operating systems and network services.

This guide prepares the TOE for operation according to the Common Criteria configuration validated by the National Information Assurance Partners (NIAP).

This guide is applicable to the TOE and ST referenced in Table 1 below.

Table 1 Reference information

Attribute	Description
AG Title	Cellcrypt Server Common Criteria Administrator Guide
AG Version	0.8.10
AG Reference	AG-FED-SRV-1
ST Title	Cellcrypt Server Security Target
ST Version	0.9.12
ST Reference	ST-FED-SRV-1
TOE Title	Cellcrypt Server
TOE Version	2.5.0

1.1. Audience

This document is intended for TOE administrators and assumes familiarity with the Cellcrypt Server or similar Internet-based enterprise telephony services. Readers should also be familiar with the general concepts and technologies associated with managing hosted enterprise services including IP-based networks, TLS and X.509 certificates, Voice-over-IP telephony and Linux-based servers.

1.2. Operational Environment and Assumptions

The Cellcrypt Server is evaluated against the Network Device collaborative Protection Profile (NDcPP) and the Enterprise Session Controller Module (MOD_ESC). Only the subsystem configurations applicable to these protection profiles are described and it is assumed that the platform conforms to the following:

1.2.1. Hardware platform

Figure 1 TOE Hardware Platform

The TOE hardware consists of a Hewlett-Packard (HP) rack-mounted server with the following specifications:

Feature	Details
Server Model	HP ProLiant DL360p Gen9
Processor	2 x Intel Xeon E5-2680 V4 2.1GHz 8 Core
Chipset family	Broadwell
Memory	96GB DDR4 RAM DIMMs
Disk storage	2 x 300GB 3.5-inch SATA hot-plug disks Smart Array P440ar 12Gbps 2GB Cache RAID Controller
I/O slots	Embedded 4x1GbE Network Adapter; Serial Port Connector (Optional); 3 x PCIe 3.0 Slots; 2 x USB 3.0 Connectors; VGA Video Connector; Dedicated iLO 4 connectors; Flexible LOM bay (Optional)
Ports	Front: 2 USB; Rear: 4 USB, video (1600 x 1200), network; Internal: 1 USB, 1 SD Card
Power Supplies	2 x 800W PSUs
Form Factor	8 Bay SFF 1U Server
Dimensions	19.7 x 19 x 1.75 inches
Weight	40 pounds

The hardware manual [Ref 1] is included with the product documentation pack. the hardware manual's safety instructions, together with instructions for powering up the server should be read and understood before connecting and powering up the TOE.

1.2.2. TOE operational components

The TOE's operational environment consists of several components that fall outside the scope of the TOE. These non-TOE components consist of the following:

- Peer SIP server – The TOE may contact peer SIP servers from other networks over a TLS-secured link for Switch-to-Switch communications.
- Remote Audit server – The TOE can send audit logs to a remote syslog server.
- NTP Server – The TOE can contact a remote NTP timestamp server with over a TLS-secured link.
- Push Server. The TOE can send push notifications to mobile client devices by connecting to a Push Service over a TLS-secured link.

2. ADMINISTRATIVE ROLES

There are three administrative roles associated with the TOE. If more administrators are required OS groups will be used to restrict roles.

- Network Administrator
- System Administrator
- User Administrator

2.1. Network Administrator

The Network Administrator is responsible for the physical management of the TOE including:

- Taking delivery of the TOE.
- Installing the TOE in the server facility including power and network connections.
- Setting up the required non-TOE remote services (see 1.2.2),
- Setting up the TOE IP addresses, DNS entries, and firewall access rules.
- Booting the TOE operating system and observing the POST and self-test results.
- Setting up the System Administrator account with remote SSH access.

The TOE is delivered with a default root admin account. After booting the TOE, the Network Administrator must immediately replace the default credentials and create an account for the System Administrator. This is done locally using a screen and keyboard. The Network Administrator sets up the System Administrator account with a default username and password and this includes setting up remote SSH access for the System Administrator. The remote access interface uses the OpenBSD version of OpenSSH and is set up according to the procedure in the TOE Installation Manual [Ref 3].

2.2. System Administrator

The System Administrator is responsible for the general management and security of the TOE via the remote SSH network interface. The System Administrator is responsible for:

- Configuring the TOE services with the domain addresses provided by the Network Administrator.
- Generating X.509 certificate requests, obtaining and installing the certificates from the designated Certificate Authority (CA).
- Configuring the login warning banners.
- Setting up the User Administrator access to the web portals.
- Initiating the TOE self-tests.
- Performing TOE software updates.
- The general security configuration of the TOE

The System Administrator also acts as the Security Administrator for the TOE.

2.3. User Administrator

The User Administrator is responsible for setting up the telephony user network via the TOE web portals. The User Administrator is responsible for:

- Adding additional User Administrators with limited controls.
- Administering user licenses.
- Adding/removing/editing user profiles, user groups, and organisation sub-domains.
- Setting user permissions to telephony and messaging services.
- Managing user devices.
- User support e.g. password resets.

The User Administrator can only administer the services provided by the TOE web portals. The User Administrator does not have an account on the TOE operating system and cannot perform TOE management functions.

3. PACKAGING AND DELIVERY OF THE TOE

The TOE was delivered to the testing facility in its HP hardware packaging by a Cellcrypt employee and it contained documentation including the serial number of the device (AGD_PRE.1-1). The TOE arrived configured with a default root admin account which the Network Administrator immediately replaced.

4. TOE CONFIGURATION

The TOE configuration is carried out by the System Administrator.

4.1. Remote Administrator Access

After receiving the default SSH access details from the Network Administrator, the designated System Administrator immediately changes the account password (see 4.2.2) and SSH settings. The following settings are immediately configured by the System Administrator:

- Cryptography settings
- Warning banner

4.1.1. Cryptography settings

OpenSSH is configured to use the Cellcrypt CCoreV4 FIPS 140-2 module for all cryptographic operations. The configurable cryptographic algorithms and protocols are listed in Table 2.

Table 2 SSH Cryptographic algorithms and protocols

Cryptography type	Available algorithms and protocols
Signing	• ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521
Encryption	• aes128-ctr • aes256-ctr
Key Exchange	• ecdh-sha2-nistp256 • ecdh-sha2-nistp521
Integrity Check	• hmac-sha2-256 • hmac-sha2-512

The allowed algorithms and protocols set by the organisation security policy can be configured in the `sshd` configuration file `/etc/ssh/sshd_config`. Note: Only the listed algorithms in Table 2 are allowed for NIAP compliance. There are no SSH “none” algorithms available in the SSH library and the elliptic curve type is configurable by the algorithm selection. There is no authentication fallback function on the SSH channel.

These configurations require a local ECDSA key to be generated. For example, to generate a 521-bit ECDSA key (that’s 521, not 512), the following command can be used. The command will prompt you to save the file and enter a password for the key (the password can be left blank).

```
$ ssh-keygen -t ecdsa -b 521
```

With the local key now generated, the following example shows the changes that can be made in the `sshd` configuration file:

/etc/ssh/sshd_config

```
HostKey /etc/ssh/<ECDSA_KEY>

RekeyLimit 1G 3600s
ClientAliveInterval 3600

MACs hmac-sha2-256,hmac-sha2-512
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-
nistp521
Ciphers aes128-ctr,aes256-ctr
KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

Note `RekeyLimit` and `ClientAliveInterval` in the config file `/etc/ssh/sshd_config` limits the session key usage to no longer than one hour and no more than one gigabyte of data (required to satisfy FCS_SSHS_EXT.1.8).

After these configurations have been completed, the `sshd` service must be restarted with the following command:

```
$ systemctl restart sshd
```

4.1.1.1. Warning Banner

The warning banner is displayed whenever accessing the TOE via the remote administrator interface. It is configured in the `/setup/master.yml` file according to the procedure in the TOE Maintenance Manual [Ref 4]. A default warning banner is also displayed on the TOE web portal login screens, and this can be changed using the procedure under “Defining the timeout and warning Banner” in the TOE Maintenance Manual [Ref 4].

4.1.1.2. Failure handling

If the SSH service fails for any reason, first make sure that you have correctly configured the service (see `/etc/ssh/sshd_config`). Then, try restarting the service (as above). If this is the first-time usage, make sure that the Network Administrator has correctly configured the service. These measures should correct most failure conditions. If the failure of the SSH service persists please contact Cellcrypt Technical Services.

4.2. Security Management Functions

4.2.1. Certificates and Domains

4.2.1.1. Certificates

All certificates required for the Cellcrypt services should be placed under the `/certs` directory. We are assuming the use of a single certificate with a DNS entry in the ***subjectAltName*** (SAN) for all stack services. We are also assuming `toe-server` is the base name for all certificates. Note that the base name is specified by the `basename` parameter in the `/setup/master.yml` config file. The expected file names for the certificates are therefore:

- toe-server.pem → server certificate (leaf)

- toe-server-chain.pem → full certificate chain - must include the certificate above
- toe-server.key → certificate private key
- toe-client-root.pem → client certificate checking will be enforced by the SIP server. This file should contain the certificate used to sign the client certs (i.e. the certificates that clients will send to the server)
- toe-server-root.pem → (optional) root certificate if using self-signed certificates or authorities not trusted by the OS
- toe-client.pem → client certificate used when connecting to external servers.
- toe-client.key → client certificate key used when connecting to external servers.

Certificate validation is done by the CCoreV4 FIPS-140-2 validated module and all FIA_X509_EXT.1.1 requirements for extendedKeyUsage validation are supported. Certificate revocation is supported for external server certificates on all outgoing connections using both OCSP (RFC 6960) and CRL (RFC5759) methods. If certificate validation or revocation checking cannot be completed for any reason, the default action is to reject the certificate and terminate the connection. There are no configurable overrides or fallback functions for this action.

4.2.1.2. Domains

The TOE domains must be configured in the `/setup/master.yml` config file (see "Changing the domain and TLS certificates" in the TOE Maintenance Manual [Ref 4]).

4.2.1.3. Generating new keys and certificate requests

The `csr-req.sh` script in the `/certs` directory can be used to generate new keys and new certificate request files. The `csr-req.sh` script, makes use of the `/certs/server.cnf` and `/certs/server.cnf` config files to output Certificate Signing Requests (CSR's) that can be used to obtain a new client and server certificate. The server CSR includes the DNS entries for all the services to be included in the SAN certificate.

```
$ cd /certs
$ ./csr-req.sh server
$ ./csr-req.sh client
```

The output files `/certs/server-csr.pem` and `/certs/client-csr.pem` can be forwarded to a CA to obtain the certificates.

If the keys and/or certificate are generated elsewhere, then they need to be copied directly into the `/certs` folder and should be named exactly as shown above. Note that the server certificate **toe-server-chain.pem** should contain the server certificate plus the intermediate CA certificate/s appended in chained order.

Note: When generating keys for the XMPP service the returned certificates and key should be copied over the default keys in /var/lib/prosody.

4.2.1.4. Diffie-Hellman keys

To replace the default nginx Diffie-Hellman key use the following command:

```
$ openssl dhparam -out /etc/nginx/ssl/dhparam.pem 2048
```

To replace the default XMPP Diffie-Hellman key use the following command

```
$ openssl dhparam -out /var/lib/prosody/dhparam-2048.pem 2048
```

4.2.1.5. Erasing keys

The following list of keys are used on the TOE:

- /certs/toe-client.key
- /certs/toe-server.key
- /var/lib/prosody/xmpp-server.key
- /etc/nginx/ssl/dhparam.pem
- /var/lib/prosody/dhparam-2048.pem

Previously used keys can be erased using an appropriate file wipe utility. We recommend installing the Red Hat scrub package:

```
$ yum install scrub
```

The scrub utility overwrites files with NNSA NAP-14.1-C patterns before deleting the file e.g:

```
$ scrub /certs/toe-server-key.pem
```

Note that the TOE specifies hard drives and not SSDs so that there is no delay in file erasure at the physical layer. If Solid State Drives (SSDs) must be used instead, then we recommend that the SSD's must be destroyed by incineration when being replaced (see also section 4.2.8).

4.2.1.6. Elliptic curve selection

The default elliptic curve is set to the NIST P-384 curve and will be used with all algorithms requiring elliptic curve computations. With SSH operations the elliptic curve used (NIST-only) depends on the algorithm selection (see section 4.1.1).

4.2.2. Password policy

4.2.2.1. Password Management

According to FIA_PMG_EXT.1.1 in the TOE Security Target, the TOE access passwords must conform to the following:

FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "[", "]", "{", "}", ":", ";"];
- Minimum password length shall be configurable to between 9 and 20 characters

By default, the TOE operating system (RHEL 7.6) accepts any printable characters from the ASCII list as a valid password character.

To enforce the use of at least one of each class (digit, upper case, lower case, and special character) and a minimal length of 9~20, modify the file `/etc/security/pwquality.conf`. See example below:

/etc/security/pwquality.conf

```
minlen = 9
minclass = 4
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
```

The `minlen` parameter determines that the minimum password length and can be modified to a value between 9 and 20. The `minclass` parameter determines that it should contain at least one character from each of the four available classes: digit, upper case, lower case, and others/special characters.

4.2.3. Access Restriction

To restrict access to TOE after 6 login attempts, modify both `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` with the following lines:

/etc/security/pwquality.conf

```
auth    required      pam_faillock.so preauth silent audit deny=6 unlock_time=300
auth    [default=die]  pam_faillock.so authfail audit deny=6 unlock_time=300
account required pam_faillock.so
```

These parameters should be located correctly in the file. Please refer to the following image for correct placement.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faillock.so preauth silent audit deny=6 unlock_time=300
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        [default=die]  pam_faillock.so authfail audit deny=6 unlock_time=300
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so
account     required      pam_faillock.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok


password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

After the maximum login tries is reached the administrator is locked out for a period of 300 seconds after which time the account will again become unlocked. The following log is emitted at `/var/log/secure`.

/var/log/secure

```
2021-01-05T12:21:01.348471-05:00 api-niap unix_chkpwd[7475]: password
check failed for user (devops)
2021-01-05T12:21:01.349083-05:00 api-niap sshd[7464]:
pam_faillock(sshd:auth): Consecutive login failures for user devops
account temporarily locked
```

Passwords can be reset using the TOE operating system commands e.g.:

```
$ passwd sysadmin
```

Type your current user password when prompted, type the new password when prompted and finally, retype the new password when prompted.

4.2.4. Warning banners

There are two sets of TOE access warning banners

- SSHD warning banner
- Portal warning banners

The SSHD warning banner configuration is described in section 4.1.1.1 and the portal warning banners configurations are described in section 4.3.5.

4.2.5. Session Idle Timeout

According to FTA_SSL_EXT.1.1, The TSF shall, for local interactive sessions, terminate the session after a Security Administrator-specified period of inactivity. Note: The TOE System Administrator also acts as the Security Administrator.

To set the value for this inactivity period, add or edit the value of `TMOUT` of the following files:

- `/etc/profile`
- `<USER_HOME_DIR>/.bash_profile`
- `<USER_HOME_DIR>/.bashrc`

The `/etc/profile` file is a configuration set for all users of the system. Changing this file means that all the logins made into the TOE will follow the configuration rules and scripts set in this file.

The other user configuration files are for a user's home directory and are specific to that user. These are also listed here to allow specifying a timeout for a specific user.

The `TMOUT` parameter uses seconds to set the timeout. Setting its value to 300 means that it will wait for 300 seconds (5 minutes) before closing a local or remote session. Be sure that

the variable `TMOUT` is exported and is set as `readonly`, so that any other user is not able to edit it.

Example:

```
...
TMOUT=300
readonly TMOUT
export TMOUT
...
```

Any changes regarding the session idle timeout will only take effect with the next user login. For this reason, it is recommended that, after any changes, the user sign out and then sign in again to the TOE.

For remote sessions, the configurations for `sshd` should also be changed (see 4.1).

To terminate the remote access session normally type the following command:

```
$ exit
```

4.2.6. Start-up Tests

To conform with SFR FPT_TST_EXT.1.1 and FPT_FLS.1.1 the TOE can perform a series of self-tests (see Self-Tests in the TOE Maintenance Manual [Ref 4]). To change the behaviour on self-test fail modify the `systemctl` command parameter in the python script `/etc/startup-tests`. The default behaviour is to force the TOE operating system into `rescue` mode. If the start up tests fail and rebooting does not restore operation please contact Cellcrypt Technical Support.

4.2.7. Software updates

Software updates are managed by the System Administrator and performed according to the procedure under the heading “Installing the Stack” in the TOE Installation Manual [Ref 3]. After installation the TOE stack version can be found in the VERSION file stored under the `/opt/secure` folder by executing the following command:

```
$ cat /opt/secure/VERSION
```

4.2.8. Secure Disk Erasure

The TOE hardware platform (HPE DLP360 Gen9 server) is supplied with a comprehensive built-in diagnostic and troubleshooting utility called “Intelligent Provisioning”. This utility also provides support for secure erasure of the hard disks. See “Secure Disk Erasure” in the TOE Maintenance Manual [Ref 4]. Note: The TOE hardware platform does not support the TRIM command when Solid State Disks (SSD’s) are used instead of hard drives. For guaranteed destruction of SSD’s, the System Administrator must physically destroy the SSDs by incineration. This can be carried out by an authorised data destruction service.

4.2.9. Status of VVoIP endpoints

The System Administrator can monitor the status of VVoIP endpoints by monitoring the endpoint activity on the remote audit server. Each time an endpoint registers/terminates a connection with the ESC or makes/disconnects a call, an ESC event log is automatically triggered and can be viewed in real time on the remote audit server.

4.3. Configuration of services

4.3.1. NTP Service

The online timestamp servers use the Network Transport Protocol (NTP). Broadcast and multicast NTP packets are disabled by default. If required, then cryptographic authentication is also required. The NTP client configuration can be modified to include a secure timestamp service based on HMAC-SHA256 authentication. For basic configuration see “NTP” in the TOE Installation Manual [Ref 3]. For secure timestamp see “Authenticated NTP setup” in the TOE Maintenance Manual [Ref 4]). Any NTP configuration changes will require a restart of the NTP service. To restart the NTP service:

```
$ systemctl restart ntpd.service
```

4.3.1.1. Failure handling

All NTP service failures will be logged, and additional failure instructions can be found in section 4.4.2.

4.3.2. Enterprise Session Controller

The Enterprise Session Controller (ESC) is implemented using the well-known OpenSIPS software. The OpenSIPS configuration file is stored in **`/etc/secure-conf/opensips.cfg`**. However, most of the details in this configuration file are populated automatically during installation or upgrading of the TOE software via the `/etc/master.yml` file (see TOE Installation Manual [Ref 3]. Only the cipher-suites are manually updated in the **`/etc/secure-conf/opensips.cfg`** file (see section

4.3.2.1. Endpoint authentication

ESC endpoint connections require mutual authentication and therefore all ESC endpoints require X.509 client certificates. The client certificate CommonName (CN) is compared to a client domain name specified by the `clientCertDomain` parameter in the `/setup/master.yml` file. ESC endpoint authentication configuration is described under “Appendix XIII - Enable SIP Mutual Authentication” in the TOE Installation Manual [Ref 3].

4.3.2.2. Restarting the ESC service

Any direct configuration changes to `/etc/secure-conf/opensips.cfg` will require a restart of the ESC services. To restart the ESC services directly:

```
$ systemctl restart opensips
$ systemctl restart sip-reverse
```

Any changes to `/etc/master.yml` will reguire restarting the service using the following command:

```
$ /setup/setup.sh -r sip
```

4.3.2.3. Failure handling

ESC service failures will be logged, and in most cases may simply require a restart of the service as shown above. Additional instructions for handing ESC failures can be found in section 4.4.4

4.3.3. XMPP Service

The XMPP service is supported using the Prosody XMPP server to receive XMPP messages via the server-to-server (s2s) interface. It can also be enabled to allow local clients to be registered. The client TLS interfaces (5222 and 5269) conforms to FCS_TLSC_EXT.1 in the NDcPP and the s2s TLS server interface conforms to FCS_TLSS_EXT.1.

4.3.3.1. Prosody configuration changes:

The Prosody configuration does not allow individual TLS cipher-suite selection so we must use the "openssl ciphers" style to tailor TLS cipher-suites to meet FCS_TLSC_EXT.1.1 and FCS_TLSS_EXT.1.1. The following configuration changes are required in the file `/etc/prosody/prosody.cfg.lua`

/etc/prosody/prosody.cfg.lua

```
-- This ssl parameter group is used for the user server with XMPP clients
ssl = {
        key = "/var/lib/prosody/xmpp-server.key";
        certificate = "/var/lib/prosody/xmpp-server-chain.pem";
        cafile = "/var/lib/prosody/xmpp-rootca-chain-cert.pem";

           ciphers  =  "HIGH:ECDH+AES:-DES:-3DES:-RC4:-SHA:-MD5:-DSS:-aDSS:-ADH:-
aECDH:-CAMELLIA128:-CAMELLIA256:-aNULL:-aDH";

        dhparam = "/var/lib/prosody/dh_2048.pem";
}

log = {
    -- Log files (change 'info' to 'debug' for debug logs):
    debug = "/var/log/prosody/prosody.log";
    error = "/var/log/prosody/prosody.err";
    -- Syslog:
    {
        levels = { "error" };
        to = "syslog";
    };
}

-- These are for the s2s settings
VirtualHost "xmpp-toe.cellcrypt.com"
       enabled = true

    ssl = {
        key = "/var/lib/prosody/xmpp-server.key";
        certificate = "/var/lib/prosody/xmpp-server-cert-chain.pem";
        -- Note: Use "capath: instead of "cafile" if the s2s servers are public or from
other domains
        -- capath = "/etc/pki/ca-trust/source/anchors";
        cafile = "/var/lib/prosody/xmpp-rootca-chain-cert.pem";

           ciphers = "HIGH:ECDH+AES:-DES:-3DES:-RC4:-SHA:-MD5:-DSS:-aDSS:-ADH:-aECDH:-
CAMELLIA128:-CAMELLIA256:-aNULL:-aDH";

        dhparam = "/var/lib/prosody/dh_2048.pem";
}
```

Notes:

1. Generate the `dhparam` in the following way:

```
$ openssl dhparam -out /var/lib/prosody/dhparam-2048.pem 2048
```

2. The default `capath` parameter (commented out with --) is used if the external client/server is using a public CA. If not, use the `capath` or `cafile` parameter to point to a specific CA cert that can be used to validate the external client/server.

Any changes made to the `/etc/prosody/prosody.cfg.lua` file will require a restart of the XMPP service. To restart the XMPP service:

```
$ systemctl restart prosody.service
```

4.3.3.2. Failure handling

XMPP service failures will be logged, and in most cases may simply require a restart of the service as shown above. Additional instructions for handing XMPP service failures can be found in section 4.4.3

4.3.4. TLS Interfaces

All TOE cryptography uses OpenSSL's FIPS 140-2 validated algorithms. The following cipher-suites are the only ones allowed by FCS_TLSC_EXT.1 in the NDcPP. The IANA mappings are included (https://testssl.sh/openssl-iana.mapping.html).

4.3.4.1. Cipher-suites

Table 3 lists the TLS cipher-suites supported by the TOE.

Table 3 TLS Cipher-suites

OpenSSL names	IANA names	IANA codes
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256	0x003c
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256	0x003d
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384	0x009d
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256	0x009c
DHE-RSA-AES128-SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067
DHE-RSA-AES256-SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006b
DHE-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009e
DHE-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009f
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xC023
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xC024
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC02B
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC02C
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xc027
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xc028
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030

4.3.4.2. Changing TLS cipher-suites

The above supported TLS cipher-suites are configured, by default for all TLS services. To change the cipher-suites used by a particular service, the relative service's configuration file must be modified. For more details see "Changing TLS cipher-suites" in Cellcrypt Maintenance

Manual [Ref 4]. Details for configuring the client certificate for a remote ESC is described in section 4.4.4.

4.3.5. Enterprise Management Portal (EMP)

The Enterprise Management Portal (EMP) is the main administration portal allowing subscribers of the Enterprise Session Controller (ESC) to be registered in the database. The only configuration item applicable here is the warning banner and the login timeout. The default values are:

- Enterprise Portal Idle timeout: 20 minutes.
- Enterprise Warning Login Banner: "ALERT! You are entering into a secured area. All connections are monitored and recorded. Please disconnect immediately if you are not an authorized user. Unauthorized access will be fully investigated and reported to the appropriate law enforcement agencies."

To change any of these values, edit the corresponding fields within the file:

/etc/nginx/conf.d/emp.ini

```
[auth]
lifetime=

[secure-emp]
warningbanner=
```

If left empty, the default values will be used.

The MY portal can optionally be used by telecom users to change their passwords and view their registration details. Changes to portal configuration will require a restart of nginx:

```
$ systemctl restart nginx
```

4.3.5.1. Failure handling

Portal failures will be logged and if the service fails to respond, in most cases this may require a restart of `nginx` as shown above. If the portal services do not resume after restarting `nginx` please contact Cellcrypt Technical Support.

4.3.6. Enterprise Communication Service (ECS)

The Enterprise Communication Service (ECS) uses Asterisk for conferencing services. The Asterisk instance configuration file can be found at:

`/etc/asterisk/secure_gateway_federal.conf`.

It is automatically populated by the ECS installer based on the master configuration file `master.yml` (see TOE Installation Manual [Ref 3]).

4.3.6.1. Restarting the ECS Secure Gateway

If any changes are manually applied to `secure_gateway_federal.conf`, the Asterisk service must be restarted. As root, run:

```
$ systemctl restart asterisk-sg
```

4.3.6.2. Failure handling

ECS service failures will be logged, and in most cases may simply require a restart of the `asterisk-sg` service as shown above. If the ECS portal fails to respond, try restarting `nginx`:

```
$ systemctl restart nginx
```

If none of these measures restore ECS service please contact Cellcrypt Technical Services.

4.3.7. Auxiliary Service

The Auxiliary service (AUX) provides access to miscellaneous information for the client devices which is not yet available from the Cellcrypt Server's API service. Updates to the software on the server may not occur as frequently as with the client devices. The AUX service allows administrators to provide information required by the client devices, such as the latest client version number available for download. Client devices will regularly check for updates using the AUX service. Device version files are located at `/opt/secure/aux/appinfo/<platform>`, where `<platform>` can be either `Android`, `Windows`, or `iOS`. Copy the version json files into their correct directories when they become available from Cellcrypt under the appropriate platform folder as the appropriate bundle id (e.g. android/com.csg.federal for the Android Client). Note: Restart nginx after making changes.

To test - point your browser to: https://aux.domain.com/appinfo/<platform>/com.csg.federal

Output (example only): `{"version": "10.0.0"}`

4.3.7.1. Restarting the Aux service

When making changes to the config file above, be sure to restart `nginx`:

```
$ systemctl restart nginx
```

4.3.7.2. Failure handling

The Aux service does not have an associated portal. Most service failures are likely to be associated with missing files in the download directories. Please make sure that there is an entry for each platform under the `/opt/secure/aux/appinfo/` or try restarting `nginx` as shown above.

4.3.8. RNG service

The Random Number Generation (RNG) functionality is provided by the underlying Cellcrypt CCorev4 FIPS 140-2 module's DRBG and is not configurable by the TOE.

4.3.9. Auditing Service

The TOE provides extensive logging facilities, supporting both local logging and secure remote logging of events. The audit logs consist of both local logs and remote logs. Local logs are protected using the TOE operating system directory permissions.

4.3.9.1. Overview

The TOE's auditing system makes use of the `auditd` and `rsyslog` services.

4.3.9.1.1. auditd

The `auditd` service is the user space component of the Linux Auditing System responsible for writing audit records to the disk. Viewing the logs is done using the `ausearch` or `aureport` utilities. Configuring the audit rules is done using the `auditctl` utility. The audit daemon's configuration options are found in the `/etc/audit/auditd.conf` file.

4.3.9.1.2. rsyslog

The `rsyslog` service is an advanced central logging service based on the original `syslog`, which served as a standard for sending and receiving notification messages in a particular format from various network devices. The messages include time stamps, event messages, severity, host IP addresses, diagnostics and more. There are eight severity levels numbered 0 - 7 with 0 being the highest severity (Emergency) ranging down to warning and informational levels, and finally, 7 is reserved for debug messages. The `rsyslog` service is configured using the configuration files `/etc/rsyslog.conf` and optionally, `/etc/rsyslog.d/*.conf`. The `rsyslog` service can transfer log data to multiple destinations, including remote servers. When the IP and port for a remote audit server is defined, `rsyslog` transfers data from Syslog to a local port open by Stunnel, which is responsible for establishing a secure TLS link with the remote audit server (see section 4.3.9.16). Further details on `rsyslog` can be obtained in the TOE Installation Manual [Ref 3] under Audit Module).

4.3.9.1.3. nftables

The `nftables` service is the new packet classification framework that replaces the existing `{ip,ip6,arp,eb}_tables` infrastructure. It is possible to create network rules for income and outcome connections. For audit purposes, it can be used to log all the IPv4 and IPv6 connections. The configurations for `nftables` are stored on `/etc/nftables.conf`.

4.3.9.1.4. ntpstat

The `ntpstat` service will report the synchronisation state of the NTP daemon running on the local machine. If the local system is found to be synchronised to a reference time source,

`ntpstat` will report the approximate time accuracy, the pooling frequency, and the IP address of the NTP server. The polling rate is of 1024 seconds.

4.3.9.2. Log rotation

FAU_STG_EXT mandates that the server should provide appropriate measures to preserve the logs when the server's storage capacity is exceeded. The TOE uses a rotation log system with archive compression.

For `auditd` the following parameters must be present in the `/etc/audit/auditd.conf` file:

/etc/audit/auditd.conf

```
flush = INCREMENTAL_ASYNC # instructs the service to flush records to
disk when "freq" number is reached
freq = 50
max_log_file = 8 # max number of log files on server
num_logs = 5 # number of log files to keep if rotate is given as the
max_log_file_action = ROTATE
```

For `rsyslog` the following parameters must be present in the config files under /etc/logrotate.d:

/etc/logrotate.d/*

```
weekly # rotate log files weekly
rotate 4 # keep 4 weeks-worth of backlogs
compress # compressed log files
```

4.3.9.3. Access control

FAU_GEN.1/Log and FAU_SAR.1/Log dictate that the access to the audit trails must be limited to a list of authorized users, and that they are protected from unauthorized modifications, disclosure, or deletion. In the default configuration, both the audit services selected require Administrator privileges to successfully access files.

In addition, Administrator sessions are also monitored/audited to prevent ill-intended modifications to audit trails.

4.3.9.4. Start-up/shutdown date/time of audit functions

FAU_GEN.1.1 mandates that the TOE shall generate an audit record of the start-up and shutdown of the audit functions. Both `auditd` and `rsyslog` are managed by `systemctl` on RHEL 7.6 and configuring `journalctl` to output to `/var/log/messages` fulfils the requirement.

Example output for startup:

```
Jul 23 14:49:36 ip-172-31-33-210.us-west-2.compute.internal systemd[1]:
Starting Security Auditing Service...
Jul 23 14:49:36 ip-172-31-33-210.us-west-2.compute.internal
auditd[22693]: Started dispatcher: /sbin/audispd pid: 22695
Jul 23 14:49:36 ip-172-31-33-210.us-west-2.compute.internal
auditd[22693]: Init complete, auditd 2.8.4 listening for events (startup
state enable)

Jul 30 12:52:34 ip-172-31-33-210.us-west-2.compute.internal systemd[1]:
Starting System Logging Service...
Jul 30 12:52:34 ip-172-31-33-210.us-west-2.compute.internal
rsyslogd[24806]: [origin software="rsyslogd" swVersion="8.24.0-34.el7"
x-pid="24806" x-info="http://www.rsyslog.com"] start
Jul 30 12:52:34 ip-172-31-33-210.us-west-2.compute.internal systemd[1]:
Started System Logging Service.
```

Example output for shutdown:

```
Jul 23 14:49:34 ip-172-31-33-210.us-west-2.compute.internal
auditd[2207]: The audit daemon is exiting.
```

4.3.9.5. IP connections

FAU_GEN.1.1/Log states that the TSF shall be able to generate a system log record of IP connections. The file `/etc/nftables.conf` configures the firewall `nftables` to enable logging of IP connections:

/etc/nftables.conf

```
table inet filter {
    chain INPUT {
        type filter hook input priority 0; policy accept;
        ip saddr != 127.0.0.1 ct state new counter log prefix "New
Connection: "
        ip6 saddr != ::1 ct state new counter log prefix "New
Connection: "
        icmp type echo-request counter log prefix
"LOG_IPTABLES_PING_REQUEST: "
    }
    chain FORWARD {
        type filter hook forward priority 0; policy accept;
    }
    chain OUTPUT {
        type filter hook output priority 0; policy accept;
        ip daddr != 127.0.0.1 ct state new counter log prefix "New
Connection: "
        ip6 daddr != ::1 ct state new counter log prefix "New
Connection: "
    }
}
```

The configuration above output any IP connections directly into the syslog file.

Example output for IP Connections:

```
Aug 5 19:07:41 ip-172-31-33-210 kernel: LOG_IPTABLES_PING_REQUEST: IN=eth0 OUT=
MAC=06:d6:65:61:b7:fe:06:b1:01:79:45:47:08:00 SRC=179.184.19.129
DST=172.31.33.210 LEN=84 TOS=0x00 PREC=0x00 TTL=38 ID=6627 DF PROTO=ICMP TYPE=8
CODE=0 ID=32536 SEQ=200

Aug 5 19:07:42 ip-172-31-33-210 kernel: LOG_IPTABLES_PING_REQUEST: IN=eth0 OUT=
MAC=06:d6:65:61:b7:fe:06:b1:01:79:45:47:08:00 SRC=179.184.19.129
DST=172.31.33.210 LEN=84 TOS=0x00 PREC=0x00 TTL=38 ID=6791 DF PROTO=ICMP TYPE=8
CODE=0 ID=32536 SEQ=201

Aug 5 19:07:43 ip-172-31-33-210 kernel: LOG_IPTABLES_PING_REQUEST: IN=eth0 OUT=
MAC=06:d6:65:61:b7:fe:06:b1:01:79:45:47:08:00 SRC=179.184.19.129
DST=172.31.33.210 LEN=84 TOS=0x00 PREC=0x00 TTL=38 ID=6835 DF PROTO=ICMP TYPE=8
CODE=0 ID=32536 SEQ=202
```

Note: Per FAU_GEN.1/CDR's test no. 1, the IP connections are tested through the "ping" command (hence the log format shown above).

4.3.9.6. Miscellaneous status logs

FAU_GEN.1.1/Log also calls for disk and file storage capacity, NTP status, CPU usage, memory usage, audit storage capacity and fan status. The evaluation tests revolve around monitoring said parameters for a 10-minute period and performing calls/messaging. These are handled using a simple shell script to forward the outputs from existing OS monitoring services. The OS utility `top` is used for CPU/memory status, and `df`, for available disk space. These outputs are redirected to the `syslog` log file `/etc/audit/hardwFeed.sh`

/etc/audit/hardwFeed.sh

```
#!/bin/bash

for COMMAND in "df -h" "ntpstat" "sensors" "top -b | head"
do
   $COMMAND | logger -s -t "${COMMAND}"
done
```

The above script is fed to the service `hardwFeed.service` which is executed every minute (per ESC requirements) by `hardwFeed.timer` ensuring the info is logged every minute.

4.3.9.7. Example outputs

Disk/file storage capacity:

```
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: Filesystem Size Used Avail Use%
Mounted on
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: /dev/xvda2 10G 3.4G 6.7G 34% /
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: devtmpfs 897M 0 897M 0% /dev
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 919M 0 919M 0% /dev/shm
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 919M 79M 840M 9% /run
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 919M 0 919M 0%
/sys/fs/cgroup
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 184M 0 184M 0%
/run/user/1000
Aug 5 18:55:01 ip-172-31-33-210 journal: df -h: tmpfs 184M 0 184M 0%
/run/user/0
```

NTP Status:

```
Aug 5 18:55:01 ip-172-31-33-210 ntpstat: synchronised to NTP server
(204.11.201.10) at stratum 3
Aug 5 18:55:01 ip-172-31-33-210 ntpstat: time correct to within 37 ms
Aug 5 18:55:01 ip-172-31-33-210 ntpstat: polling server every 1024 s
```

CPU/Memory usage:

```
Aug 6 14:41:54 ip-172-31-33-210 top: top - 14:41:54 up 19 days, 3:04, 2 users,
load average: 0.00, 0.01, 0.05
Aug 6 14:41:54 ip-172-31-33-210 top: Tasks: 182 total, 2 running, 180 sleeping,
0 stopped, 0 zombie
Aug 6 14:41:54 ip-172-31-33-210 top: %Cpu(s): 0.0 us, 6.2 sy, 0.0 ni, 93.8 id,
0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Aug 6 14:41:54 ip-172-31-33-210 top: KiB Mem : 1880524 total, 64660 free,
1247988 used, 567876 buff/cache
Aug 6 14:41:54 ip-172-31-33-210 top: KiB Swap: 0 total, 0 free, 0 used. 352988
avail Mem
Aug 6 14:41:54 ip-172-31-33-210 top: mbie
Aug 6 14:41:54 ip-172-31-33-210 top: PID USER PR NI VIRT RES SHR S %CPU %MEM
TIME+ COMMAND
Aug 6 14:41:54 ip-172-31-33-210 top: 21324 ec2-user 20 0 162028 2104 1540 R 6.2
0.1 0:00.01 top
Aug 6 14:41:54 ip-172-31-33-210 top: 1 root 20 0 128148 5032 2504 S 0.0 0.3
4:03.70 systemd
Aug 6 14:41:54 ip-172-31-33-210 top: 2 root 20 0 0 0 0 S 0.0 0.0 0:00.36
kthreadd
```

4.3.9.8. Local Administrative Logins

The first item of FAU_GEN.1.1 states that all administrative login and logout events must be accounted for, as well as the start/stop of trusted channels. The TOE handles this by setting watching rules on login/logout binaries, which, in addition to "`aureport -l`" functionality, produces reports on all login attempts on the server. The `aulast` package is used for trusted channels initiation/termination info. Additionally, `rsyslog` is configured to audit all attempts to initiate a super-user session (including commands such as sudo).

Login configuration and info:

```
-w /etc/login.defs -p wa -k login
-w /etc/securetty -p wa -k login
-w /var/log/faillog -p wa -k login
-w /var/log/lastlog -p wa -k login
-w /var/log/tallylog -p wa -k login
```

Example output:

Login info:

```
Login Report
============================================
# date time auid host term exe success event
============================================
1. 08/06/2019 15:50:09 ec2-user 200.175.61.81.static.gvt.net.br
/dev/pts/0 /usr/sbin/sshd yes 919456
2. 08/06/2019 18:13:41 ec2-user 200.175.61.81.static.gvt.net.br
/dev/pts/0 /usr/sbin/sshd yes 919808
3. 08/07/2019 09:17:17 ec2-user 200.175.61.81.static.gvt.net.br
/dev/pts/0 /usr/sbin/sshd yes 921179
4. 08/07/2019 13:24:55 ec2-user 200.175.61.81.static.gvt.net.br
/dev/pts/0 /usr/sbin/sshd yes 921613
5. 08/07/2019 13:27:52 ec2-user 200.175.61.81.static.gvt.net.br
/dev/pts/0 /usr/sbin/sshd yes 921820
6. 08/07/2019 14:46:53 ec2-user 200.175.61.81.static.gvt.net.br
/dev/pts/0 /usr/sbin/sshd yes 924724
7. 08/07/2019 16:05:17 ec2-user 200.175.61.81.static.gvt.net.br
/dev/pts/0 /usr/sbin/sshd yes 926211
```

Trusted channel info:

```
ec2-user pts/0 179.184.19.129.s Mon Aug 5 18:16 - 19:58 (01:41)
ec2-user ssh 200.175.61.81.st Mon Aug 5 20:27 - 20:27 (00:00)
ec2-user pts/2 200.175.61.81.st Mon Aug 5 19:24 - 22:42 (03:17)
ec2-user pts/5 200.175.61.81.st Mon Aug 5 19:52 - 23:59 (04:06)
ec2-user pts/2 200.175.61.81.st Tue Aug 6 14:28 - 14:38 (00:09)
ec2-user pts/0 179.184.19.129.s Tue Aug 6 14:20 - 14:43 (00:23)
ec2-user pts/2 200.175.61.81.st Tue Aug 6 14:38 still logged in
```

Super-user sessions:

```
Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_unix(sudo:session): session
opened for user root by ec2-user(uid=0)
Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_tty_audit(sudo:session):
unknown option `ec2-user'
Aug 8 20:40:20 ip-172-31-33-210 sudo: pam_tty_audit(sudo:session):
changed status from 1 to 1
Aug 8 20:41:39 ip-172-31-33-210 sudo: pam_unix(sudo:session): session
closed for user root
Aug 8 20:41:54 ip-172-31-33-210 sudo: ec2-user : TTY=pts/0 ;
PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/systemctl restart rsyslog
```

4.3.9.9. Bad SSH Authentication

FAU_GEN.1.1 also requires the TOE to log unsuccessful login attempts, including when they exceed some preset limit. The TOE uses `auditd`'s own summary reporting plugin - `aureport` - and through specifying auditing rules for the `pam_tty` service.

4.3.9.10. Audit configuration

```
$ aureport -i -au --failed
```

Example output:

```
Authentication Report
============================================
# date time acct host term exe success event
============================================
1. 07/31/2019 12:29:42 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 845672
2. 07/31/2019 13:12:40 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 845839
3. 07/31/2019 13:31:19 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 845872
4. 07/31/2019 19:01:13 ec2-user 200.175.61.81 ssh /usr/sbin/sshd no 848199
5. 07/31/2019 19:28:00 ec2-user 179.184.19.129 ssh /usr/sbin/sshd no 848260
```

4.3.9.11. Changes to Time and Date

The FPT_STM_EXT.1 requirement makes it necessary to audit any discontinuous changes in time. Monitoring time-related binaries and executables (see example below) audit any attempts to discontinuous time changes on the TOE server.

```
-a always,exit -F arch=b32 -S settimeofday,adjtimex,clock_settime -F key=time
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -F key=time
-w /etc/localtime -p wa -k localtime
```

4.3.9.12. Audit configuration

Example output:

```
Executable Report
===================================
# date time exe term host auid event
===================================
332. 08/06/2019 13:23:34 /usr/lib/systemd/systemd ? ? unset 877714
333. 08/06/2019 13:23:34 /usr/lib/systemd/systemd-timedated (none) ? unset
877713
334. 08/06/2019 13:23:34 /usr/lib/systemd/systemd-timedated (none) ? unset
877715
335. 08/06/2019 13:24:04 /usr/lib/systemd/systemd ? ? unset 877716
336. 08/06/2019 13:25:45 /usr/lib/systemd/systemd ? ? unset 877729
337. 08/06/2019 13:25:45 /usr/bin/timedatectl pts0 ? ec2-user 877726
338. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset
877728
339. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset
877731
340. 08/06/2019 13:25:45 /usr/lib/systemd/systemd-timedated (none) ? unset
877732
```

Summary report of executables involved in changing TOE server's timezone:

4.3.9.13. Manual Update Attempts

FMT_MOF.1/ManualUpdate mandates that all attempts to initiate a manual code update must be audited. Even though FPT_TUD_EXT.1 events are no longer needed to be audited (initiation/result of update attempts), logging the outputs of the manual updates fulfils both requirements.

4.3.9.14. Call Detail Records

The protected local logs include the Call Detail Records (CDR's). These permissions are automatically set during the TOE software installation process. The CDR's are generated by the ESC OpenSIPS service and consist of the following information:

- TOE unique identifier
- Call originator identifier
- Call receiver identifier
- Unique transaction sequence number
- Call status (missed / connected / terminated / failures)
- Call type (voice / voice + video)
- Call start time
- Call end time
- Call duration
- Call direction (incoming / outgoing)
- Call routing into TOE
- Call routing out of TOE
- Time zone

Example call log showing CDR details:

```
2022-02-18T19:17:55.672734+00:00 sip-alpha /usr/local/sbin/opensips[35710]: ACC:
call ended:
created=1645211866;call_start_time=1645211867;duration=8;ms_duration=8296;setupt
ime=1;method=INVITE;from_tag=fa6f84b3-38a2-4709-8ffd-
3e10f52df51d;to_tag=809ab268-06ba-41e1-9f03-4270ebe692af;call_id=ba07fafd-963c-
4639-a454-
6bba4627c887;code=200;reason=OK;src_ip=;dst_ip=13.90.174.9;call_end_time=1645211
875;call_type=Audio;caller=;callee=
```

4.3.9.15. Audit configuration

Direct modifications to the setup script were made to log all update messages prompted. E.g.:

```
echo "$(good ${service}): Running precondition checks." | logger -s -t "SW
upgrade"
check-pre
fail-if-needed
echo "$(good ${service}): Configuring system." | logger -s -t "SW upgrade"
configure
fail-if-needed
echo "$(good ${service}): Starting services." | logger -s -t "SW upgrade"
run
fail-if-needed
echo "$(good ${service}): Running final checks." | logger -s -t "SW upgrade"
check-post
fail-if-needed
echo "$(good ${service}): Installed." | logger -s -t "SW upgrade"
```

Example output:

```
Aug 6 18:31:54 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m:
Running precondition checks.
Aug 6 18:32:50 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m:
Running precondition checks.
Aug 6 18:32:50 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m:
Configuring system.
Aug 6 18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m:
Starting services.
Aug 6 18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m:
Running final checks.
Aug 6 18:32:53 ip-172-31-33-210 journal: SW upgrade: #033[1;32mmariadb#033[0m:
Installed.
```

4.3.9.16. Audit server settings

The default port for the remote audit server is 11514. To change the default port and set the IP value, please edit the following section of `/setup/master.yml`:

/setup/master.yml

```
network:
...
  remote_auditing:
    host_name: REMOTE_AUDIT_SERVER_HOST_NAME
    port: REMOTE_AUDIT_SERVER_PORT
...
```

Replace `REMOTE_AUDIT_SERVER_HOST_NAME` and `REMOTE_AUDIT_SERVER_PORT` with the appropriate information.

To update the audit system with the new remote audit server settings, please run the audit setup with the reconfigure option:

```
$ /setup/setup.sh -r audit
```

4.3.9.17. Failure handling

If the audit service fails, first check that your configuration changes (above) are correct. Next, try to restart the associated services:

```
$ systemctl restart stunnel
$ systemctl restart rsyslog
$ systemctl restart auditd
```

If the audit services still fail to operate correctly, please contact Cellcrypt Technical Services.

4.4. Remote server access

The TOE can make secure connections with the following remote servers:

- Remote Audit server
- Remote NTP server

- Remote XMPP server
- Remote ESC (SIP server)

4.4.1. Remote Audit Server

The remote audit server connection details are configured by modifying the default IP address and port number in the file `/setup/master.yml` under `network:` (see section 4.3.9.16).

If the remote audit service fails for any reason, please check that the remote audit server is running and that its IP address and port have not changed. Also confirm that the configuration settings above match the actual IP address and port number of the remote audit server. To restart the service after making any changes:

```
$ /setup/setup.sh -r audit
```

4.4.2. Remote NTP server

The TOE can synchronise its clock with several remote NTP servers. It can also connect to authenticated NTP services. NTP timestamps can be authenticated using HMAC-SHA26 based on a 256-bit secret key (see TOE Maintenance Manual for more details [Ref 4]).

If the NTP service fails for any reason, please consult the NTP server section in the TOE Maintenance Manual for more guidance or try restarting the service using the following command:

```
$ systemctl restart ntpd.service
```

4.4.3. XMPP Server

The XMPP outgoing connection is configured in the second `ssl` block in the `/etc/prosody/prosody.cfg.lua` file (see 4.3.2).

If this connection fails, check the clients are using the correct remote domain in the outgoing messages (The XMPP service routes to external XMPP servers based on the outgoing server domain name in the messages (like with email). To restart the service, use the following command:

```
$ systemctl restart prosody
```

4.4.4. Remote ESC

The ESC can also connect to remote ESC's with TLS mutual authentication. The remote ESC domain is configured in `/setup/master.yml` by the User Administrator. The remote domain details are added under `external_hosts:` (see TOE Installation Manual [Ref 3]). Note: you will need to contact the Network Administrator to add a DNS entry for each external host listed under `external_hosts` see example below showing an entry for an external `sip2` host:

/etc/master.yml

```
services:
...
  sip:
...
    external_hosts:
      sip2:
        hostname: sip2-niap.cellcrypt.com
        commonname: sip2-niap.cellcrypt.com
        alias: sip2
        ip: 34.212.64.69
        port: 5061
        cert: "/certs/certsandkeys/client1@sip-niap-cert.pem"
        key: "/certs/certsandkeys/client1@sip-niap-key.pem"
```

The local ESC looks for outgoing calls to any of the configured remote ESC's and when these are detected, the local ESC makes a server-to-server (s2s) call to the remote ESC. This involves a TLS mutual authenticated connection. The TOE uses its configured client certificate for mutual authentication. The TOE will not accept incoming calls from any remote ESC other than the ones configures under `external_hosts` in the `/setup/master.yml` file.

To enable the changes after editing `/setup/master.yml` execute the following command:

```
$ /setup/setup.sh -r sip
```

If the ESC remote interface fails for any reason, check that the correct domain has been registered in the `/setup/master.yml` file. Reconnecting to the remote ESC generally requires simply making a call to the correctly configured remote ESC host.

5. USER NETWORK MANAGEMENT

The telephony user network is managed by the User Administrator using the TOE web portals. Although these portals can be used over the Internet, we recommend that they are only accessed via the organisation's internal safe network (CSfC red network). There are two web portals available:

- Enterprise Management Portal (EMP)
- Enterprise Communication Service (ECS)

5.1.1. EMP

EMP allows the User Administrator to manage the telephony and messaging user network. The portal is accessed with a browser over an HTTPS secured session. The login screen displays a configurable warning banner (see 4.3.5). The User Administrator is required to login with username and password. EMP provides the following capabilities:

- User license management.
- User registration, search, edit, delete, assign usage limits.

- Device management, view devices, last login, remote erase data.
- Domain/company segregation.
- Administrator management – Create/edit/delete, Assign roles, domains/companies.

EMP uses the TOE's central database to store usernames and device information. The ESC uses the same information to authenticate callers. More details on the EMP can be found in the Cellcrypt EMP Manual [Ref 6].

5.1.2. ECS

The ECS portal is essentially a server-side telephony client that the User Administrator can use to send messages/attachments to individual users or to groups. ECS can be used to create and manage groups, conferences and send user notifications. ECS provides the following features:

- Create user groups.
- Send messages and attachments to any user or group.
- Schedule conference calls using a calendar.
- Send pre-populated contact lists to users.

More details can be found in the Cellcrypt ECS Manual [Ref 7].

5.1.3. Troubleshooting

If any of the portals cannot be accessed, the User Administrator should first contact the Network Administrator to confirm the portal access URL. Any other issues should be addressed with the System Administrator.

6. REFERENCES

[Ref 1] HPE Proliant DLP360p Gen9 Server User Guide, Part Number: 767927-009, February 2018, Edition: 9, https://support.hpe.com/hpesc/public/docDisplay?docId=c04441974&docLocale=en_US

[Ref 2] Intelligent Provisioning User Guide for HPE ProLiant Gen9 and Synergy Servers, Part Number: 794362-008c, July 2017, Edition: 4, https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00018639en_us#erase-utility

[Ref 3] Cellcrypt Federal Stack – Installation Manual, dated February 17, 2022

[Ref 4] Cellcrypt Federal Stack – Maintenance Manual, dated February 17, 2022

[Ref 5] Cellcrypt Federal Stack – Auditing and Monitoring, dated February 22, 2022

[Ref 6] Cellcrypt Enterprise Management Portal (EMP) User Manual, Document Version 1.5, May 2020

[Ref 7] Cellcrypt Enterprise Communication Service (ECS) User Manual, Document Version 3, March 2016

7. ABREVIATIONS AND ACRONYMS

Table 4 Abbreviations and Acronyms

AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
DH	Diffie-Hellman
DNS	Domain Naming Service
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECS	Enterprise Communications Service
EMP	Enterprise Management Portal
ESC	Enterprise Session Controller
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
POST	Power On Self-Test
PP	Protection Profile
DRBG	Digital Random Bit Generator
RSA	Rivest Shamir Adleman Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation