

THALES

CTE-U Health Manager Utility

REFERENCE GUIDE



Health Manager

CTE-U Health Manager (`cte_u_manager`) is a utility that you can use to perform configuration operations and monitor the health of individual CTE-U clients. The utility is stored at `/usr/bin/cte_u_manager`. It is symbolically linked to: `/opt/vormetric/DataSecurityExpert/agent/secfs/bin/cte_u_manager`.

- [Performing Health Check](#)
- [Using the Monitor](#)
- [Service Commands](#)
- [Viewing the Service Status](#)
- [Gathering the Technical Dump](#)
- [Troubleshooting | Debugging CTE-U](#)

Utility Service Commands

```
cte_u_manager [help] [issues] [monitor] [restart] [start] [stop] [status [Path]] [techdump]
```

Command	Description
<code>help</code>	Display the <code>cte_u_manager</code> usage.
<code>issues</code>	Perform the health check. The command also reports the list of currently known issues, if any. Refer to Performing Health Check for details.
<code>monitor</code>	Start the CTE-U monitor. Refer to Using the Monitor for details.
<code>restart</code>	Restart the CTE-U service. Refer to Restarting the Service for details.
<code>start</code>	Start the stopped CTE-U service. Refer to Starting the Service for details.
<code>stop</code>	Stop the running CTE-U service. Refer to Stopping the Service for details.
<code>status</code>	Show the overall configuration and health status of CTE-U. You can also use this command to view the status of individual

Command	Description
	encrypted directories. Refer to Viewing the Service Status for details.
techdump	Gather useful data about your system. Thales Customer Support might seek this information for troubleshooting any problems you might experience with CTE-U. Refer to Gathering the Technical Dump for details.

Performing Health Check

Run the `issues` command to perform a health check of the local CTE-U software. If no problems are detected, `There are 0 issues` is displayed. It indicates a healthy system. However, if any issues are detected (that is, the system is sick), the number of issues with additional details about each issue is displayed.

Healthy

For example, if no issues are detected:

```
sudo /usr/bin/cte_u_manager issues
There are 0 issues
```

Sick

For example, if some issues are detected:

```
sudo /usr/bin/cte_u_manager issues
There are 2 issues
keyManager: connect() failed.
gdb (PID 97446) is attached to 100611.
```

Using the Monitor

Run the `monitor` command to view and/or modify the log level and other configurations interactively. To use the monitor:

```
sudo /usr/bin/cte_u_manager monitor
```

The main monitor console appears, as shown below.

```
CTE-Userspace Health Manager 17:07:10 Status: Good
OS Version: CentOS Linux 7 Kernel Version: 3.10.0-693.el7.x86_64
CTE Version: cte_fuse-9.1.0.000-237.x86_64 CTE Install Date: Mon 28 Dec 2020 12:23:27 PM EST
Key Manager Connection Status: Good
Systemctl Status: Active: active (running) since Mon 2020-12-28 12:45:19 EST; 4h 21min ago

Control Plane
  PID  PPID  TYPE  THREADS  FDS  TIME  CPU %  VM SIZE  VM RSS
AGENT  52715  1     N/A     20      10    04.7   0.00    1.1G   4.9M
FUSE PARENT  52707  1     N/A     2       7    01.5   0.00    200.6M 101.7M

Data Plane
  PID  PPID  TYPE  THREADS  FDS  TIME  CPU %  VM SIZE  VM RSS
/home/testuser/encrypted  52735  52707  Local    5      9    00.1   0.00    297.6M  4.1M
/mnt/nfs1                  100675 52707  NFS      6      9    00.2   0.00    369.7M  3.6M
/mnt/nfs2                  100611 52707  NFS      6      9    00.4   0.00    433.7M  4.5M

Press 'h' for help, 'x' to exit
```

Monitor Syslog Service

When the CTE-U Health Manager is running in the `monitor` mode, any issues are logged to the configured Syslog server. For example, if you attach a debugger to one of the `secfs_fuse` processes, then when it detaches it from the process, the following messages are logged to the Syslog server:

```
Dec 29 06:56:42 localhost cte_u_manager[28394]: Error: gdb (PID
28628) is attached to 100675.
Dec 29 06:56:52 localhost cte_u_manager[28394]: Recovered: gdb (PID 28
628) is attached to 100675.
```

Service Commands

Starting the Service

The `start` command runs `/etc/cte/secfs start`, and then waits until the CTE-U service is up and running. This includes waiting for the encrypted directories to be mounted (something `systemctl` does not do). If CTE-U is already running, the `start` command is not applicable.

Note

The start command is blocked until CTE-U is completely started and initialized. As long as `cte_u_manager` detects any internal issues (refer to [Performing Health Check](#) for details), it is blocked and waits for the issues to resolve. That makes the start command preferable over `systemctl start cte_u_manager`, especially, if you are running it from a tool that expects CTE-U to be completely up and running when the command returns.

The following console output shows how `systemctl start cte_u_manager` returns before the CTE-U service is completely up and running.

```
sudo systemctl start secfs-fuse ; sudo /usr/bin/cte_u_manager issues
| head -1
There are 44 issues
```

The following console output shows how the start command waits until CTE-U is completely up and running before it returns.

```
sudo /usr/bin/cte_u_manager start ; sudo
/usr/bin/cte_u_manager issues | head -1
There are 0 issues
```

The following sequence of commands shows the start command is not applicable if CTE-U is already running:

```
sudo systemctl status cte_u_manager | grep Active:
Active: inactive (dead) since Tue 2020-12-29 10:29:51 EST; 9min ago
sudo /usr/bin/cte_u_manager start
sudo systemctl status cte_u_manager | grep Active:
Active: active (running) since Tue 2020-12-29 10:39:10 EST; 6s ago
sudo /usr/bin/cte_u_manager start
sudo systemctl status cte_u_manager | grep Active:
Active: active (running) since Tue 2020-12-29 10:39:10 EST; 15s ago
```

Stopping the Service

The `stop` command runs the `/etc/cte/secfs stop` command internally, and then remains blocked and waits until CTE-U is completely shut down. It is essentially the same as the `/etc/cte/secfs stop` command. The `stop` command is provided for the sake of creating a complete set of `stop`, `start`, and `restart` commands.

Restarting the Service

The `restart` command restarts the CTE-U service. This command has the same effect as running the `stop` command followed by the `start` command.

The `restart` command is similar to, but not identical to, running the `/etc/cte/secfs restart` command. The difference is that the `restart` command returns as soon as the CTE-U Agent and `secfs_fuse` "parent process" are up and running.

If you have a set of encrypted directories, they probably are not protected immediately after the `systemctl` command returns. The `restart` command, on the other hand, blocks until all the encrypted directories are protected.

Therefore, if you have an automated tool that starts CTE-U and expects the encrypted directories to be protected, the `restart` command is a better choice than `/etc/cte/secfs restart`.

An example of the `restart` command is shown below:

1. Check the status of the CTE-U service.

```
sudo systemctl status secfs-fuse | grep Active:  
Active: active (running) since Tue 2020-12-29 09:30:29 EST; 45min  
ago
```

The output shows that the service has been running for 45 minutes.

2. Restart the CTE-U service.

```
sudo /usr/bin/cte_u_manager restart
```

3. Recheck the status of the CTE-U service.

```
sudo systemctl status secfs-fuse | grep Active:
Active: active (running) since Tue 2020-12-29 10:17:21 EST; 39s a
go
```

The output shows the CTE-U service is restarted and has been running for 39 seconds.

Viewing the Service Status

Run the status command to view the overall health status of CTE-U. The command can be run with or without an argument.

No Arguments

If you run the status command with no arguments, the utility dumps a set of configurations and status information to the console.

For example:

```
sudo /usr/bin/cte_u_manager status
```

Response

```
OS_VERSION="Ubuntu 20.04.5 LTS"
KERNEL_VERSION="5.4.0-128-generic"
CTE_VERSION="10.0.0.41"
CTE_INSTALL_DATE="2022-11-18 17:04:27"
SYSTEM_STATUS="Sick"
SYSTEM_STATUS_NUM_ISSUES=1
```

The output is divided into **two** parts:

- **Versions** of the OS and CTE-U. For example:

```
OS_VERSION="Ubuntu 20.04.5 LTS"
KERNEL_VERSION="5.4.0-128-generic"
CTE_VERSION="10.0.0.41"
CTE_INSTALL_DATE="2022-11-18 17:04:27"
```

- **Quick status** of the CTE-U software. If no issues are detected, the console output shows the system as Healthy and the reported issues as zero (0). For example:

```
SYSTEM_STATUS="Healthy"  
SYSTEM_STATUS_NUM_ISSUES=0
```

If any issues are detected, the console output shows the system as Sick and the number of reported issues. For example:

```
SYSTEM_STATUS="Sick"  
SYSTEM_STATUS_NUM_ISSUES=2
```

One Argument

The argument is either:

- Pathname of a GuardPoint
- Pathname of a file in an encrypted directory

If you specify the name of a GuardPoint, it displays the status of only the GuardPoint:

```
$ sudo /usr/bin/cte_u_manager status /opt/test1
```

Response

```
FULL_PATHNAME="/opt/test1"  
PROTECTED_DIRECTORY="/opt/test1"  
PROTECTED_DIRECTORY_STATUS="Healthy"
```

If you specify the name of a file in a GuardPoint, it displays the status of the file:

```
$ sudo /usr/bin/cte_u_manager status /opt/test1/finances.txt
```

Response

```
FULL_PATHNAME="/opt/test1/finances.txt"  
PROTECTED_DIRECTORY="/opt/test1"  
PROTECTED_DIRECTORY_STATUS="Healthy"
```



```
RELATIVE_PATH="finances.txt"
RELATIVE_PATH_ENCRYPTED="true"
```

Gathering the Technical Dump

Use the `techdump` command to gather useful data about your system. Thales Customer Support might seek this information for troubleshooting any problems you might experience with CTE-U.

The dump file is created in the `/var/log/vormetric` directory (or a different directory specified using the interactive installer). The name of the file is listed immediately after the `techdump` command starts running.

Every OS distribution stores data in its own chosen locations, therefore, the tool attempts to look around and find the data. RHEL, SUSE, and Ubuntu are all different.

For example:

```
sudo /usr/bin/cte_u_manager techdump
```

Response

```
Creating techdump file >/var/log/vormetric/
cte-2022_10_19_02_49_25-techdump.tar.bz2
Saving all system information to file: /var/log/vormetric/sysinfo/
cte-fuse-sysinfo.
Date : 2022_10_19_02_49_25
CTE-FUSE Version: 10.0.0.9013
Saving CTE-FUSE service status.
Saving OS Version.
Saving Kernel Version.
Saving VM status.
Saving disk info.
Collecting /proc/partitions to sysinfo file.
Collecting /proc/modules to sysinfo file.
Collecting /proc/mounts to sysinfo file.
Collecting /proc/cpuinfo to sysinfo file.
Collecting /proc/meminfo to sysinfo file.
Collecting network interfaces info.
```

```
Saving firewall status.
Collecting /proc/version to sysinfo file.
Saving gcc version.
Saving the list of running processes.
Saving disk space information.
Saving dmesg logs.
Saving the system fstab file.
Saving the system mtab file.
Copying config file.
Copying syslog file.
Copying messages file.
Copying CTE-FUSE log files.
Create tar file.
Remove temporary directory ... Done.
Successfully created techdump file.
```

The sample output shows the techdump file is created. If needed, you can share the technical dump file with Thales Customer Support. To view the details of the file, run:

```
sudo ls -lh /var/log/vormetric/cte-2022_10_19_02_49_25-techdump.t
ar.bz2
-rw-r--r-- 1 root root 90K Oct 19 02:50 /var/log/vormetric/cte-202
2_10_19_02_49_25-techdump.tar.bz2
```

Troubleshooting/ Debugging CTE-U

This topic is for collecting information for the Support team so that they can help you resolve your issues as efficiently as possible. When you talk to a Support Engineer, they will request this information. Thales recommends gathering this information before calling them.

Warning

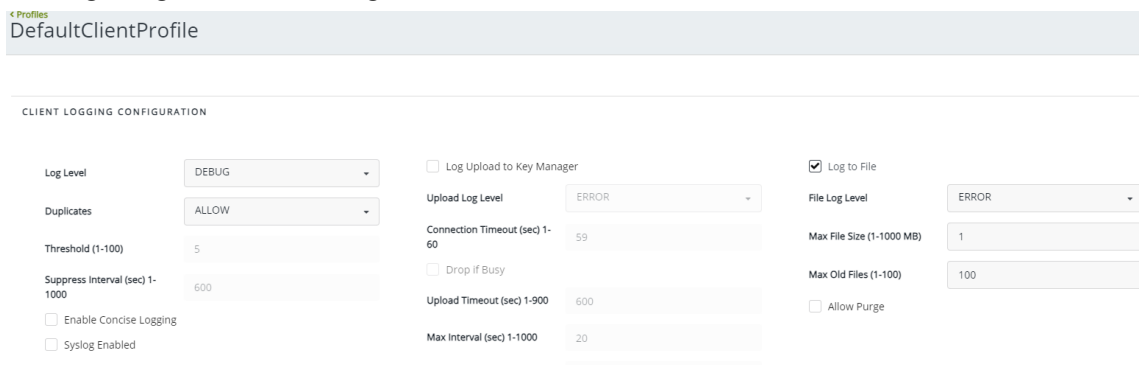
Before enabling logs, configure syslog settings to disable rate limiting.

Application level logs for VMD

- By default, VMD stores its logs in `/var/log/vormetric/vorvmd_root.log`

To enable the logs:

1. Go to the appropriate CipherTrust Manager client profile.
2. Click **CLIENT LOGGING CONFIGURATION**.
3. Change log level to debug.



Profiles
DefaultClientProfile

CLIENT LOGGING CONFIGURATION

Log Level	DEBUG	<input type="checkbox"/> Log Upload to Key Manager	<input checked="" type="checkbox"/> Log to File
Duplicates	ALLOW	Upload Log Level	ERROR
Threshold (1-100)	5	Connection Timeout (sec) 1-60	59
Suppress Interval (sec) 1-1000	600	<input type="checkbox"/> Drop if Busy	
<input type="checkbox"/> Enable Concise Logging		Upload Timeout (sec) 1-900	600
<input type="checkbox"/> Syslog Enabled		Max interval (sec) 1-1000	20
		File Log Level	ERROR
		Max File Size (1-1000 MB)	1
		Max Old Files (1-100)	100
		<input type="checkbox"/> Allow Purge	

Filesystem level logs

The filesystem information defaults to the syslog file which defaults to:

RHEL, SLES, Oracle Linux, Amazon Linux

```
/var/log/messages
```

Debian

```
/var/log/syslog
```

To enable the FS logs through either `secfsd` or `voradmin`:

1. For persistent logs (persist even after service restart) enable with `voradmin`:

```
voradmin secfs config debug_all {4-8} <GuardPoint>
```

2. Restart CTE-U:

```
/etc/cte/secfs restart
```

To set the logs for the current life cycle of the SecFS service, use secfsd:

```
secfsd -log_level {4-8} <GuardPoint>
```

Note

- Use the option to enable the logs for a specific GuardPoint. Otherwise, it is not needed.
- Four is the default value. It indicates that logging is off.
- Eight is the max value. It indicates the highest debug logging.

Collecting System Information

The debugging steps for CTE-U require collecting system information about the system/OS that is running.

To automatically collect all of the information and create a log file at `/var/log/vormetric/cte-xxxxx`:

- Type:

```
/usr/bin/cte_u_manager techdump
```

Collecting CipherTrust Manager Information

1. Collect the policy information like key name and key type.

key Version 0 +

ID	cd713093_d4c2bc35	Owner	local\admin	Object Type	Symmetric Key
UUID	7b2562e0_223622f2	Created	15 Apr 2024, 09:29	Algorithm	AES
MUID	7b2562e0_223622f2	Last Modified	15 Apr 2024, 09:30	Size	256
KeyID		Exportable	<input checked="" type="checkbox"/>	Deleteable	<input type="checkbox"/>
XTS/CBC CS1	False	Global Usage	<input type="checkbox"/>	Key Check Value	894bdc

KEY GENERAL

KEY ACCESS

General NAE

Key Owner
admin [Change](#)

Search groups
2 Results | 2 groups Show All Groups

Group	Read	Use	Upload	Decrypt	Encrypt	Sign	Verify	MAC	MACVerify	Export	All
admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CTE Clients	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2 groups 5 per page

2. In **Policies > Policy Elements**, collect the resource set name and corresponding definition.

3. In **Policies > Policy Elements**, collect the user set name and corresponding definition.

4. Capture the **Settings > Profiles** details.

RANSOMWARE PROTECTION CONFIGURATION

Trusted Process Set

Select process set [Select](#) [X](#)

Operation
Block

[Update](#)

MULTIFACTOR AUTHENTICATION

Select ODC Connection
Select ODC Connection [X](#)

Select MFA Exempted User Set
Select Userset [X](#)

The selected user set will be exempted from MFA enforcement. MFA will not be enforced on the users of this set.

[Update](#)

5. Click on the appropriate Client and collect the GuardPoint status information.

GuardPoints Client Settings Membership Challenge Response

Refresh GuardPoints

2 Total GuardPoints 0 Inactive 0 Disabled 2 Active 0 Unknown

Protected Path Search by Protected Path

0 Selected 0 Results | 2 GuardPoints [Create GuardPoint](#)

Status	Policy Name	Protected Path	Type	Client Group	Enabled	LDT Progress	Multifactor Authentication
<input checked="" type="checkbox"/> Active	abc	/GSP	Auto Directory	-	Yes	N/A	<input type="checkbox"/>
<input checked="" type="checkbox"/> Active	abc	/hana	Manual Directory	-	Yes	N/A	<input type="checkbox"/>

2 GuardPoints 10 per page

Support Contacts

If you encounter a problem while installing, registering, or operating the product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at [Thales Customer Support](#), is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

Tip

You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@Thales.com.