THALES

CTE-U Agent Advanced Configuration Guide for Linux

CTE-U 10.3.0

Using CTE-U with Linux

- Overview of CTE UserSpace
- Getting Started
- Special Cases for CTE UserSpace Policies
- Logging
- Enhanced Encryption Mode
- CTE with systemd
- Utilities
- Upgrading CTE UserSpace
- Uninstalling CTE UserSpace

CTE-U Overview

CTE-U is a file-system level transparent encryption solution that leverages the cryptographic and key management features of the CipherTrust Manager platform to protect unstructured data. CTE UserSpace performs transparent encryption: authorized users and processes continue to have read and write access to the encrypted data; unauthorized users and processes cannot access the encrypted data.

CTE UserSpace provides data security with fully automated encryption of unstructured data contained on file servers and network shares. Working together with a CipherTrust Manager appliance, CTE UserSpace uses policies to protect the folders and files residing on servers and network shares.

CTE UserSpace now also offers block level encryption.

While handling a file, CTE-U does not encrypt, modify, or update most file metadata, such as file name, creation time, type, size, ownership, or attributes. Exceptions are:

- **Time stamp**: When CTE-U transforms a folder, each file’s time stamp is updated when the transformation is complete.
- **File size as seen by Backup users**: Backup users see the actual size of the encrypted file. Other users see the pre-encryption size of the file.

The Security Officer administers the policies and keys on the CipherTrust Manager Console. The administrator deploys CTE UserSpace on servers and network shares. CTE UserSpace protects the specified local paths and mapped network shares. The server sends the logs and notifications to CipherTrust Manager. Users accesses the files from the server as per the applied access policies.

Getting Started

This section describes how to install CTE for Linux, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following topics:

- Configuring CTE-U with CipherTrust Manager
- Additional Considerations

Configuring CTE-U with CipherTrust Manager

This section describes how to install and configure CTE on Linux systems that you plan to register with a CipherTrust Manager.

Configuration Overview

The configuration process when you are using CTE UserSpace with a CipherTrust Manager consists of the following steps:

1. Install and register CTE on the protected host as described in the CTE UserSpace Installation Guide.

2. You can also install CTE-U in silent mode.

3. Note that you can use External Certificates for communication between CTE and CM. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

Enhanced Encryption Mode

This section describes the enhanced AES-CBC-CS1 encryption mode for keys. It contains the following topics:

- Disk Space
- File Systems Compatibility

- Using the AES-CBC-CS1 Encryption Mode in CipherTrust Manager

CTE with systemd

CipherTrust Transparent Encryption (CTE) for Linux is integrated with the systemd framework. To ensure that applications start after the CTE agent starts at startup, you must modify `systemd`. This is also true when the CTE agent is started and stopped manually.

This section contains the following topics:

- Overview of CTE and systemd
- CTE Agent Control Changes on systemd
- CTE Configuration Changes Required on systemd
- Supported Use Cases

CTE Agent Control Changes on systemd

The commands to start, stop, restart, and check CTE status on `systemd` are shown in the following table.

Command	Command syntax for distributions that support systemd
Start	`/etc/vormetric/secfs start`
Restart	`/etc/vormetric/secfs restart`
Stop	`/etc/vormetric/secfs stop`
Check status	`/etc/vormetric/secfs status`

The normal states of CTE services on a system with one or more active GuardPoints is shown in the following list. It is normal for `secfs-fs` to be listed as active (exited).

- `secfs-fuse`: active (exited) state

Example

To check the status of CTE, type:

```
    /etc/vormetric/secfs status
```

Response

```
    secfs-fuse service: active (running) since Tue 2022-09-27 09:51:
04 CDT; 1h 3min ago
```

> **Note**
>
> `/etc/vormetric` is a symlink to `/etc/cte`. You can use them interchangeably in CTE UserSpace.

Utilities

Thales provides a variety of utilities that augment the standard Linux utilities. This combination of tools helps administrators manage CTE-U. The following utilities are described in this section:

- Agent Health Return Codes
- agentinfo Utility
- check_host Utility
- GuardPoint Tuning
- Nested File Systems Information
- Restricting Access Overrides with Client Settings
- register_host Utility
- secfsd Utility
- Using Advanced Encryption Set New Instructions (AES-NI)
- vmd utility
- vmsec Utility

CTE-U Linux Authentication and Client Settings

CTE UserSpace client (also known as host) settings, ensures CTE UserSpace user access controls and systems protection. This section provides a description of the client settings, authentication, and the two authenticators available with CTE UserSpace.

Root Privileges

Users with root privileges have unrestrained capabilities to override all file access and execution permissions imposed by the system. `setuid` programs running with root permissions and privileges can create, remove, or modify any files in the system. By exploiting the ability to escalate privileges, adversaries can subvert system controls and access and steal confidential data.

CTE UserSpace Access Controls

Use CTE UserSpace client access controls to:

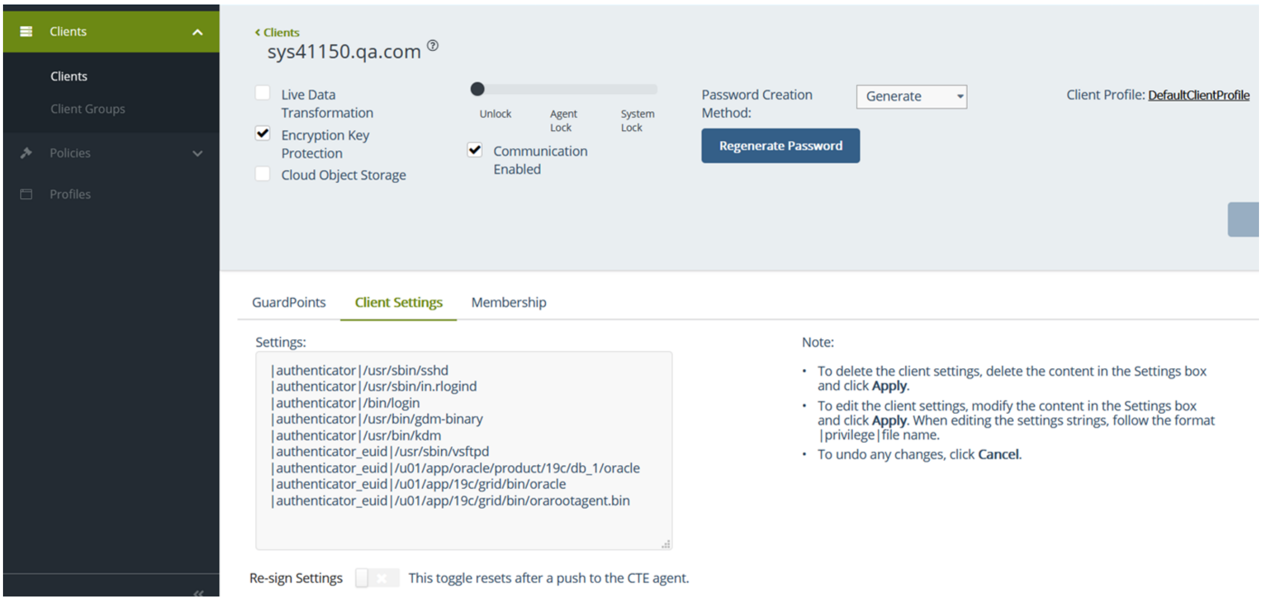
- Curtail privileges of root users and `setuid` programs.
- Specify policies to restrict "who" (the client system users or groups) and "what" (the application processes or binaries) access to protected data within CTE UserSpace GuardPoints.

By default, the CTE UserSpace Agent does NOT trust any process as authenticated. Any attempt to access a resource by any process is therefore flagged with a `User Not Authenticated` notification. Therefore, the CTE UserSpace Agent must be instructed to trust the authenticator process progeny.

CTE UserSpace client settings are the means by which an administrator configures user authorization. Client settings are tags or keywords with pipe (`|`) delimiters specifying full-system binary paths to trusted programs (referred to as authenticators) on the CTE UserSpace client. The subsequent sections describe the client settings tags, their properties and behavior, and the equivalent binaries and best practices.

Enabling CTE UserSpace Client Settings for Authenticator Programs on the CipherTrust Manager

Client settings can be enabled for individual clients or client groups with the CipherTrust Manager GUI or REST API. On the CipherTrust Manager GUI, the Client Settings tab of clients is used to configure client settings.



□ Live Data Transformation

☑ Encryption Key Protection

□ Cloud Object Storage

☑ Communication Enabled

Password Creation Method: Generate

Client Profile: DefaultClientProfile

Settings:

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator_euid|/usr/sbin/vsftpd
|authenticator_euid|/u01/app/oracle/product/19c/db_1/oracle
|authenticator_euid|/u01/app/19c/grid/bin/oracle
|authenticator_euid|/u01/app/19c/grid/bin/orarootagent.bin
```

Note:

- To delete the client settings, delete the content in the Settings box and click **Apply**.
- To edit the client settings, modify the content in the Settings box and click **Apply**. When editing the settings strings, follow the format |privilege|file name.
- To undo any changes, click **Cancel**.

Re-sign Settings This toggle resets after a push to the CTE agent.

Note

The client settings provided by the default installation are examples. **Remove** all unnecessary client settings, as they may pose security risks.

Adding, Removing, or Modifying Client Settings

When client settings are modified, verify the updated settings after a few minutes by running `secfsd -status auth`. Also, before applying new client settings, **stop** any dependent applications.

Description of Authenticators

authenticator

The `authenticator` keyword is used to specify the full path of the authenticator program authorizing the real UID of the process progeny. The real UID of the process, and its descendants, are used to set CTE UserSpace’s trusted UID. Therefore, CTE UserSpace follows and authorizes the real UID of the user authenticator process and its descendants. In general, programs that use user name and password pairs (for example, `sshd` and `login`) are candidates for being authenticators.

Example of client settings:

```
`|authenticator|/usr/sbin/sshd`
`|authenticator|/usr/sbin/in.rlogind`
`|authenticator|/bin/login`
`|authenticator|/usr/bin/gdm-binary`
`|authenticator|/usr/bin/kdm`
```

Programs that do not authenticate users should not be tagged as authenticators. Examples of such programs include `su` invoking `setuid`/`seteuid` or `setgid`/`setegid` system calls. Tagging `/usr/bin/su` with the `authenticator` keyword authorizes a root user to become a non-privileged user even without authentication. Therefore, `/usr/bin/su` should not be set as an authenticator.

`/usr/bin/su` can be set as an authenticator in cases where a root administrator legitimately uses `su` to temporarily switch privileges. Use this mode sparingly.

authenticator_euid

The `authenticator_euid` keyword works similar to `authenticator`, but instead of the real UID, the CTE UserSpace access control uses EUID for granting access. Specifically for Oracle, the database process (`oracle`) is started by the root process and then a `setuid` system call forces the service account user ID of either `oracle` or `orauser`. For such processes, CTE UserSpace should rely on the EUID of the process for authentication.

The `|authenticator_euid|` keyword is applied as follows:

```
`|authenticator_euid|/u01/app/oracle/dbhome_1/bin/oracle`
`|authenticator_euid|/u01/app/grid/bin/grid`
```

Deploying the Correct Authenticator

To authenticate users after they supplied credentials

```
    `|authenticator|<path-to-binary>/<binary-name>`
```

Start the process and run as a service account as root

```
    `|authenticator_euid|<path-to-binary>/<binary-name>`
```

Run with a specific user ID or no user ID

```
`|authenticator_euid|<path-to-binary>/<binary-name>`
```

Prevent root from becoming any other user to access data

```
`|authenticator|/usr/bin/sshd`
`|su_root_no_auth|/bin/su`
```

Individual GuardPoint Tuning

Previously, CTE-U took an all or nothing approach to tuning GuardPoints. You could tune all of the GuardPoints together, but you could not tune them individually. For example, you could turn write back cache on for all GuardPoints or none of them. Now you can turn it on or off per individual GuardPoint.

> **Note**
>
> A restart is required when you change the configuration.

SecFS changes for tuning

Set Global Configuration

- To set the configuration globally, type:

```
voradmin secfs config <config param> <config value>
```

Set Individual Configuration

- To set the configuration for individual GuardPoints, type:

```
voradmin secfs config <config param> <config value> [guardpoint path]
```

Tunable Parameters

Configurable Parameter	Configurable Value (Default)	Description	Status
allow_setfs	1	Uses FSUID to create files as root and change ownership with chmod; only applies to NFS.	Do not change
custom_cache_management	1	Allows for overriding of default caching	Do not change
debug_all	4	Debug level, can be adjusted later using `secfsd -log_level` <4-8>	Change as needed
debug_extra	0	Debug level	Change as needed
enable_xattr	0	Enables use of `xattrs` in the file system, default is off for best performance	Set to to `1` if performing a restore from CTE with `xattrs`. Set to `0` for normal CTE-U use.
fileinfo_cache_timeout	100	Amount of milliseconds to keep file attribute data in cache	Change as needed
log_level	4-8	Sets the sensitivity of the logs. Use `voradmin secfsd -log_level`	Change as needed but be mindful of performance issues
loginuid	1	Enforce loginuid. Without this set, `su` can bypass security	Change as needed
max_worker_threads	10	Maximum parallel threads allowed	Change as needed
mixed_policy	1	If mixed modes needed (ex: apply key on read, no apply key on write), set this value; it causes an extra access check	Change as needed
nfs_user	0		Change as needed

Configurable Parameter	Configurable Value (Default)	Description	Status
		UID of specific NFS user to use	
parallel_writes	1	Allows non-overlapping writes to run in parallel	Change as needed
splice	0	Allows use of splice call from FUSE	Change as needed
writeback_cache_local	1	Uses writeback cache for local file systems (extx, xfs, btrfs)	Change as needed
writeback_cache_nfs	0	Uses writeback cache for NFS	Change as needed

Warning

After changing any tunable parameter, you must restart CTE-U for the change to take effect.

Secfsd Utility

The `secfsd` utility displays the following attributes of CTE-U:

- GuardPoints defined in the **GuardPoints**
- Authentication parameters defined in the Client Settings tab
- Lock status set by enabling **FS Agent Locked** and **System Locked**
- Web destination and SSL certificate for uploading log entries
- Policies applied in the **GuardPoints** tab
- Status of required processes (`secfsd` and `vmd`)
- Version of `secfs`

The `secfsd` utility is also used to mount GuardPoints for `Directory (Manual Guard)`. Normally, CTE-U automatically mounts the `secfs` file system when you apply a GuardPoint to a directory. On Linux, the `secfsd` utility is located in

<install_dir>/secfs/.sec/bin and a symbolic link to this file is placed in `/usr/bin/secfsd`.

secfsd syntax

Command	Description
`-help`	display `secfsd` options

Status Options

Command	Description
`-status guard [-v | -tree]`	list all GuardPoints
`-status auth`	list authentication settings
`-status logger`	list logging details
`-status lockstat`	show status of system and agent lock
`-status policy`	list configured policies

Manual GuardPoint options

Command	Description
`-guard path`	manually guard path
`-unguard path`	manually unguard path
`-restart path`	restarts a crashed GuardPoint

Version option

Command	Description
`-version`	list version

Upgrading CTE-U on Linux

This section describes how to upgrade an existing CTE-U for Linux host to CTE UserSpace for Linux.

Upgrading CTE UserSpace

This section describes the generic instructions for interactively upgrading CTE UserSpace. If there are any changes to this procedure for the current release of CTE UserSpace, those changes will be documented in the CTE UserSpace Release Notes.

If you want to schedule an upgrade to occur the next time the system boots, see Scheduled Upgrade Feature.

1. Stop any application accessing files in the GuardPoint.
2. Log on to the host where you will upgrade CTE UserSpace. You must have root access.
3. Copy or mount the installation file onto the host system.
4. Start the upgrade by executing the install program for the release to which you want to upgrade. The following command upgrades the product and automatically accepts the CipherTrust Transparent Encryption License Agreement.

Default Directory

```
rpm -U <cteu-version>.<build>.rpm (Red hat)
```

Example

```
rpm -U cte-fuse_10.1.0.52.rpm
```

Non-Default

```
rpm -U <cteu-version>.<build>.rpm --relocate <default path>=<non-default path>
```

Example

```
rpm -U cte-fuse_10.1.0.52.rpm --relocate /opt/vormetric/DataSecurityExpert/agent=/cteu/agent
```

> **Note**
>
> Make sure that you install the upgrade in the same non-default directory in which you installed CTE-U.

Ubuntu

```
apt upgrade ./<cteu-version>.<build>.deb (Ubuntu)
```

Example

```
apt upgrade ./cte-fuse_10.1.0.52.deb (Ubuntu)
```

5. To verify that the upgrade was successful, use the `vmd -v` command:

```
vmd -v
Version 10
10.0.0.9074
2022-09-07 14:09:59 (CDT)
Copyright (c) 2009-2022, Thales Inc.  All rights reserved.
```

Scheduled Upgrade Feature

> **Note**
>
> Scheduled upgrade on reboot is not supported on HDFS nodes.

Warnings for CTE UserSpace for Linux

- Prior to upgrading your system, perform a backup or take a snapshot of your system.
- As with prior CTE UserSpace versions, Key Manager connectivity is required during upgrade.
- Yum updates, or OS patches, should be done prior to CTE UserSpace upgrade on reboot.
- You may see the following behavior if the upgrade on reboot fails due to a crash, or a power failure, (this is similar to a failure during a normal upgrade).
- If a crash, or power failure, occurs before the upgrade executes, the upgrade will not take place, and the currently installed CTE UserSpace version continues to run after the reboot. Restart the system to upgrade successfully.
- If a crash, or power failure, occurs during the upgrade, CTE UserSpace may enter an inconsistent state. Perform a restore from your backup, or roll back to the snapshot that you just took. Then, start the upgrade again.
- If a crash, or power failure, occurs after a successful upgrade, then the new version will run on the next reboot. No user intervention is required in this case.
- During reboot or shutdown, all applications and services dependent on CTE UserSpace services must be stopped before a scheduled update takes place. Failure to stop these services can result in an aborted scheduled upgrade during the system reboot. Examples of

situations that may cause an aborted upgrade are applications with open files in a CTE UserSpace GuardPoint, or a third party anti-virus software doing periodic scans.

For examples of how to set up CTE UserSpace start/stop dependencies with other programs, see CTE UserSpace and systemd.

Using the Scheduled Upgrade Feature

The following procedure describes how to use voradmin to schedule an upgrade that will be applied the next time the machine reboots.

1. If you want to check which version of CTE UserSpace for Linux you currently have installed, use the `vmd -v` command:

   ```
   vmd -v
   Version 10
   10.0.0.9074
   2022-09-07 14:09:59 (CDT)
   Copyright (c) 2009-2022, Thales Inc.  All rights reserved.
   ```

2. To schedule an upgrade on reboot, use the following commands:

   ```
   voradmin upgrade schedule <path_to_CTE_installer_binary>  y [-t
   <custom_extraction_path>]
   ```

   where:

   - `<path to CTE-U installer>` is the full path to the CTE UserSpace installation file for the release to which you want to upgrade.
   - `-y` is an optional parameter that automatically accepts the prompt and schedules the upgrade. If you do not specify this parameter, you must manually accept the License Agreement before the upgrade can be scheduled.

   For example, if you are upgrading to version 10.0.0.9074 and you want to automatically accept the license agreement and use a custom directory, you would type:

   ```
   voradmin upgrade schedule <path-to-CTE-U-package>  -y
   ```

3. If you want to verify that the upgrade was successfully scheduled, use the `voradmin upgrade show` command:

```
voradmin upgrade show
Upgrade on reboot is currently scheduled.
Current CTE-U version is 10.0.0.9074, upgrade on reboot scheduled
for CTE-U 10.3.0.65.
```

4. Reboot the machine, then log in and verify that the upgrade was successful.

```
vmd -v
Version 10
10.3.0.65
2022-09-07 14:09:59 (CDT)
Copyright (c) 2009-2024, Thales Inc.  All rights reserved.
```

> **Note**
>
> Appropriate logs will be logged in syslog.

Performing a Manual Upgrade When an Upgrade is Already Scheduled

If an administrator runs a manual upgrade after an upgrade has already been scheduled, the scheduled upgrade is cancelled and Manual upgrade proceeds.

To verify that the upgrade succeeded, the administrator can use the `vmd -v` command:

```
vmd -v
Version 6, Service Pack 2
7.1.0.66
2022-02-04
Copyright (c) 2009-2022, Thales. All rights reserved.
```

To cancel an existing scheduled upgrade on reboot:

```
    voradmin upgrade cancel
    Removed symlink /etc/systemd/system/multi-user.target.wants/secfs-
upgrade.service.
    Successfully cancelled upgrade on reboot
```

Uninstalling CTE-U from Linux

Considerations

- The CTE Agent must be removed from the Linux host before the host is removed from the key manager with which it is registered.
- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then run the uninstall again.
- Commands like `fuser` and `lsof` might not reveal an active GuardPoint because they detect active usage, not locked states. Although it may appear that a GuardPoint is inactive, it may be in a locked state. Under this condition, software removal may fail with an error similar to the following:

  ```
  /home: device is busy.
  ```

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:
   a. Decrypt any data you want to use after uninstall. After the CTE Agent software is removed, access to data is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.
      This decryption must be done on *every* GuardPoint on the host if you want to access all existing data on the host.

   b. Make sure the Agent and System locks have been disabled for the host.

   c. Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

d. *Do not* remove the host from the key manager yet.

3. Log on to the host as `root`.

4. Change the directory to an unguarded location (for example, /.).
   !!! caution

```
**Do not change ( `cd`) into the `/opt/vormetric` directory or in
to any directory below `/opt/vormetric`. If you run the uninstall
er from `/opt/vormetric` or any of its subdirectories, the
package removal utility may fail and return the following message:
**<br>`You are not allowed to uninstall from the /opt/vormetric
directory or any of its sub-
directories.`<br>`Agent uninstallation was unsuccessful.`
```

5. Start the uninstall. Type:

```
rpm -e cte-fuse
dpkg -r cte-fuse \\Ubuntu
```

6. Remove the host record from the key manager.

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.