THALES

CTE UserSpace Quick Installation Guide

CTE-U 10.3.0

CTE-U Quick Start Guide

This guide describes how to install, configure and use CipherTrust Transparent Encryption UserSpace to protect data on physical or virtual machines.

CTE-U protects data at rest, residing on Direct Attached Storage (DAS), Network Attached Storage (NAS) or Storage Area Networks (SAN). This can be a mapped drive or a mounted disk.

CTE-U secures data with little impact to application performance. It requires no changes to your existing infrastructure and supports separation of duties between data owners, system administrators, and security administrators.

Terminology and Components

CTE-U Terminology

The guide uses the following terminology:

Term	Description
CTE UserSpace	CipherTrust Transparent Encryption is a suite of products that allows you to encrypt and guard your data. The main software component of CTE UserSpace is the CTE UserSpace Agent, which must be installed on every host whose devices you want to protect.
CTE UserSpace Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE UserSpace Agent on the machine, you can use CTE UserSpace to protect any number of devices or directories on that machine.
key manager	

Term	Description
	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers CipherTrust Manager: a key manager for use with CTE UserSpace.
host / client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE UserSpace Agent is installed.
GuardPoint	A device or directory to which a CTE UserSpace data protection and encryption policy has been applied. CTE UserSpace will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.

CTE-U Components

The CTE UserSpace solution consists of two parts:

- The *CTE UserSpace Agent software* that resides on each protected virtual or physical machine (host). The CTE UserSpace Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE UserSpace Agent and the key manager is encrypted and secure.

  After the CTE UserSpace Agent has encrypted a device on a host, that device is called a GuardPoint. You can use CTE UserSpace to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.

- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE UserSpace Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

  CipherTrust Manager can be set up as either a security-hardened physical appliance or a virtual appliance. It provides access to the protected hosts though a browser-based, graphical user interface as well as an API and a CLI.

Install and Configure CTE-U with CipherTrust Manager

Note

CTE UserSpace is **only** compatible with CipherTrust Manager v2.10 and subsequent versions.

Follow these section in order to properly install and configure CTE-U:

1. Installation Prerequisites
2. Installation and Registration
3. Verifying Package Signatures
4. Setting the SE Linux state

Note

If installing CTE-U on SE (Security Enhanced) Linux with RHEL 9.1, you **must** set the SE Linux state.

Installation Prerequisites

This topic lists the tasks you must complete, and the information you must obtain, before installing CTE-U.

Prerequisites

Note

CTE-U v10.0.0, and all subsequent versions, support CipherTrust Manager v2.10 and all subsequent versions. It is **not** supported with previous versions of CipherTrust Manager.

Make sure you have the following information from the CipherTrust Manager Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group to which you want this client to be a part.

Packages

The following dependencies are prerequisites for a CTE-U installation.

- `libatomic1`
- `libselinux1`
- `libncurses5`

For RHEL8 and subsequent versions, the following dependency is also required:

- `libnsl.so.1`

Recommendations and Considerations

- The host on which you want to install CTE-U *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE-U to release 10.0.0 or later will fail.
- Thales recommends that you install CTE-U in the default location.
- Do not install CTE-U on network-mounted volumes such as NFS.
- Make the Installation root directory `/opt` a real directory.

Minimum System Requirements

GuardPoints	Recommended Storage
1	100 MB
10	1 GB
100	10 GB
1000	100 GB

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the CipherTrust Manager to all clients where you install CTE UserSpace.
- If the host is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

The following port information applies to both Windows and Linux systems.

Communication through a Firewall

If a protected client must communicate with CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

Communication with CipherTrust Manager

The default port for http communication between CipherTrust Manager and the CTE Agent is **443**. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

Limitations

- The Linux Kernel FUSE driver does not support `odirect + mmap` for any FUSE file systems. As such, use of `odirect + mmap` on CTE-U is not supported and attempting to memory map a file opened with the `odirect` flag will fail.

Installation and Registration

During the installation, you would be asked a series of questions. After the installation, you would be prompt to immediately register the CTE-U with a key manager. CTE-U must be registered with a key manager before you can protect any of the devices on the host.

> **Note**
>
> Do not install CTE UserSpace on network-mounted volumes like NFS.

Prerequisites

- CipherTrust Manager installed and configured. See CipherTrust Manager Documentation for more information.
- CipherTrust Manager must contain a Client Profile. See Changing the Profile for more information.
- CipherTrust Manager must contain a registration token. See Creating a Registration Token.

Procedure

1. Log on to the host where you will install the CTE UserSpace Agent as `root`. You cannot install the CTE-U Agent without `root` access.
2. Copy or mount the installation file to the host system.
3. Install CTE UserSpace:

Default Directory

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

Example

```
rpm -ivh cte-fuse_10.1.0.52.rpm
```

Non-Default

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

Example

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

Ubuntu

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

Example

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

> **Caution**
>
> **CTE-U does not support customer paths for Ubuntu installation. You must use the default path.**

4. The install script installs the CTE-U Agent software, and any missing dependencies, in either `/opt/vormetric` or your custom installation directory, and then prompts you to register the CTE UserSpace Agent with a key manager by running `/opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host`.

```
Welcome to the CipherTrust Transparent Encryption File System
Agent Registration Program.

Agent Type: CipherTrust Transparent Encryption File System Agent

Agent Version: 10.0.0.54

In order to register the CipherTrust Transparent Encryption File
System Agent with a Key Manager

1. you must know the host name of the machine running the DSM (the
host name is displayed on the Dashboard window of the Management
Console), and

2. unless you intend to use the 'shared secret' registration
method, the agent's host machine must be pre-configured on the DSM
as a host with the 'Reg. Allowed' checkbox enabled for this agent
type on the Hosts window of the Management Console.

In order to register with a Key Manager you need a valid
registration token from the CM.
```

```
Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Enter Y to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE-U.

```
For example:

Do you want to continue with agent registration? (Y/N) [Y]: Y

Please enter the primary key manager host name: 10.3.200.141:8445

You entered the host name 10.3.200.141<br>
Is this host name correct? (Y/N) [Y]: Y
```

6. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the
following
list.

[1] sys31186.qa.com
[2] 10.3.31.186

Enter a number, or type a different host name or IP address in
manually:<br>
What is the name of this machine? [1]: 2
You selected "10.3.31.186".
```

7. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
Please enter the profile name for this host: My-Profile
```

```
Please enter the host group name for this host, if any:
Please enter a description for this host: West Coast Datacenter
server 5

Token : 12345
Profile name : My-Profile
Host Group : (none)
Host description : West Coast Datacenter server 5
Are the above values correct? (Y/N) [Y]: Y
```

8. CTE-U finishes the installation and registration process.

```
Generating key pair for the kernel component...done.<br>
Extracting SECFS key<br>
Generating EC certificate signing request for the vmd...done.<br>
Signing certificate...done.<br>
Enrolling agent with service on 10.3.200.141...done.<br>
Successfully registered the CipherTrust Transparent Encryption
File System Agent with the<br>
CipherTrust Manager on 10.3.200.141.

Installation success.
```

Verifying Package Signatures

This section explains how to verify signatures of the CTE-U installer packages. After the signature is verified, CTE-U can be installed on file servers.

Verifying Signature of rpm Packages

To verify the signature of the rpm package:

1. Download the public key from the Support Portal:

> **Note**
>
> The key is named `610-000250-001_PUBLIC-GPG-CONNECTOR-SIGNING-KEY.key`.

2. Save the key on the file server, for example, at /cte/public_key.
3. Navigate to the directory where the extracted CTE-U packages are stored.
4. Import the public key into the rpm keystore, type:

```
Run rpm --import /path/to/public_key/<gpg_key>.
```

Example

```
rpm --import /cte/public_key/610-000250-001_PUBLIC-GPG-CONNECTOR-SIGNING-KEY.key
```

5. Verify the signature, type:

```
rpm -Kvv <protectfile_installer>.rpm.
```

Example

```
rpm Kvv cte_<version>-<build>.x86_64.rpm
```

The command output should contain information similar to the following:

```
cte-<version>-<build>.x86_64.rpm:
Header V3 RSA/SHA256 Signature, key ID <key_id>: OK
Header SHA1 digest: OK (<sha1_digest>)
V3 RSA/SHA256 Signature, key ID <key_id>: OK
MD5 digest: OK (<md5_digest>)
```

If the output contains Signature, key ID : OK for SHA256, the signature is verified successfully.

Verifying Signature of deb Packages

To verify the signature of the deb package:

1. Download the public key from the Support Portal:

   Note

   The key is named `610-000250-001_PUBLIC-GPG-CONNECTOR-SIGNING-KEY.key`.

2. Save the key on the file server, for example, at /cte/public_key.
3. Navigate to the directory where the extracted CTE-U packages are stored.
4. Import the public key, type:

   ```
   gpg --import /path/to/public_key/<gpg_key>
   ```

   For example, run:

   ```
   gpg --import /pf/public_key/610-000250-001_PUBLIC-GPG-CONNECTOR-SIGNING-KEY.key
   ```

5. Verify the signature, type:

   ```
   gpg -verify cte_<version>-<build>.deb.sig.
   ```

   If the output contains the text Good signature, the signature is verified successfully.

Verifying Signature of Interactive Installers

To verify the signature of the interactive installer package:

1. Download the public key from the Support Portal:

> **Note**
>
> The key is named `610-000250-001_PUBLIC-GPG-CONNECTOR-SIGNING-KEY.key`.

2. Save the key on the file server, for example, at /cte/public_key.
3. Navigate to the directory where the extracted CTE-U packages are stored.
4. Import the public key, type: (The signature cannot be verified without a valid public key.)

   ```
   gpg --import /path/to/public_key/<gpg_key>.
   ```

   For example, run:

   ```
   gpg --import /pf/public_key/610-000250-001_PUBLIC-GPG-CONNECTOR-SIGNING-KEY.key
   ```

5. Verify the signature.

   ```
   gpg -verify safenet_pf<version>-<build>.tar.gz.sig.
   ```

If the output contains a good signature, the signature is verified successfully.

Setting the SE Linux state

When installing CTE-U on SE (Security Enhanced) Linux with RHEL 9.1, you must set the SE Linux state. SELINUX can be set to any of the following three states:

- **Enforcing**: SELinux security policy is enforced.
- **Permissive**: SELinux prints warnings, but does not enforce the security policy.
- **Disabled**: No SELinux policy is loaded.

Installing CTE-U and Setting the SE Linux State

1. Check if SE Linux is in enforcing mode with the command `sestatus`.

```
[root@localhost ~] sestatus
```

Response

```
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 33
```

2. If it is in enforcing mode, set the state to permissive for installation, type:

```
[root@localhost ~] setenforce 0
```

3. Install CTE-U and register the client to CipherTrust Manager.

4. Run the following commands, in succession, to add the SELinux policy for CTE-U.

```
grep -i "comm=\"secfs_fuse\"" /var/log/audit/audit.log | audit2al
low -M secfs_fuse
semodule -i secfs_fuse.pp

grep -i "comm=\"vmd\"" /var/log/audit/audit.log | audit2allow -M v
mdpolicy
semodule -i vmdpolicy.pp
```

5. Restart the `SecFS_fuse` service and check the logs for any AVC denials in `/var/log/messages`.
   A denial for `setattr` is expected after adding a policy for `vmd`. If you see the message "SELinux is preventing" to any of the processes "secfs_fuse, vmd". Then execute the command mentioned in step 4 again.
6. Change the SE Linux status to enforcing once there are no more denials, type:

```
# setenforce 1
```

> **Note**
>
> For more information, see Setting SELinux states and modes.

Setting the SE Linux Policy Type

The SELINUX TYPE will be one of the following three values:

- **Targeted**: Targeted processes are protected
- **Minimum**: Modification of targeted policy. Only selected processes are protected.
- **MLS**: Multi Level Security protection.

The following file controls the state of SELinux on the system.

```
/etc/selinux/config
```

- Edit the `/etc/selinux/config` file to set the SE LINUX TYPE parameter to `SELINUXTYPE=targeted`.

Disabling SE Linux

In earlier Fedora kernel builds, setting SELINUX to disabled would also fully disable SELinux during the boot stage. If you need a system with SELinux fully disabled, as opposed to a system with SELinux running with no policy loaded, you need to set selinux=0 in the kernel command line. Use the Grubby CLI tool.

To set the bootloader to boot with SE Linux disabled, type:

```
grubby --update-kernel ALL --args selinux=0
```

To revert back to SELinux enabled, type:

```
grubby --update-kernel ALL --remove-args selinux
```

Guarding with CTE-U and CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

How to Protect Data with CTE UserSpace

CTE UserSpace uses policies created in the associated key manager to protect data. You can create policies to specify file encryption, data access, and auditing on specific directories and drives on your protected hosts. Each GuardPoint must have one and only one associated policy, but each policy can be associated with any number of GuardPoints.

Policies specify:

- Whether or not the resting files are encrypted.
- Who can access decrypted files and when.
- What level of file access auditing is applied when generating fine-grained audit trails.

A Security Administrator accesses CipherTrust Manager through a web browser. You must have administrator privileges to create policies using CipherTrust Manager. The CTE UserSpace Agent then implements the policies once they are pushed to the protected host.

CTE UserSpace can only enforce security and key selection rules on files inside a guarded directory. If a GuardPoint is disabled, access to data in the directory goes undetected and ungoverned. Disabling a GuardPoint and then allowing unrestricted access to that GuardPoint can result in data corruption.

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

1. Access the CipherTrust Manager domain to which the client is registered.
2. Identify or create an encryption key that CTE-U will use to encrypt the data on the device or directory.
3. For comprehensive policy information, see Managing Policies.

   Note

   For CTE UserSpace, you can only create **Standard Policies**.

4. Create a Standard GuardPoint for the device or directory.
5. Guard CTE Kernel files with CTE-U.

Access the CipherTrust Manager Domain

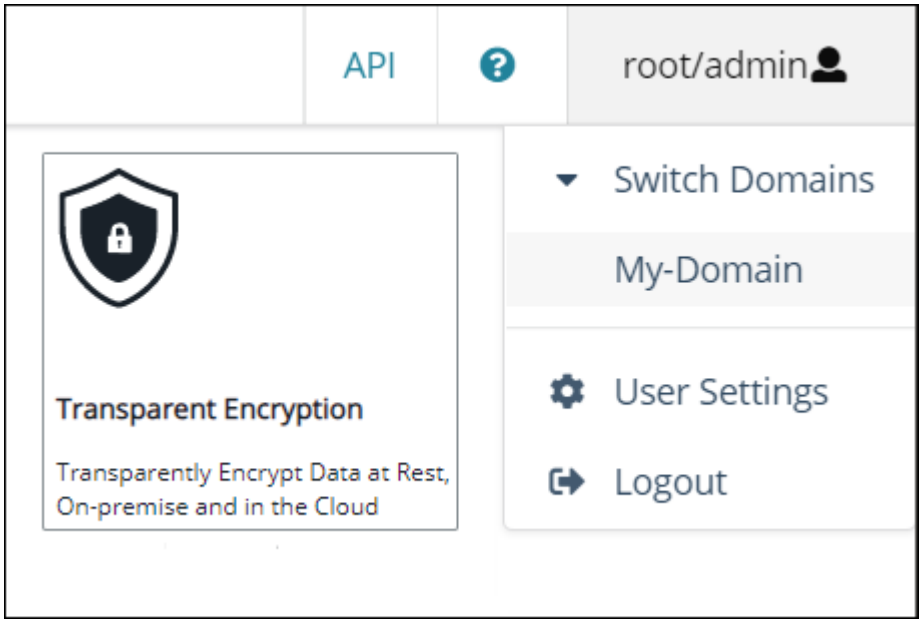
1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.

2. If the client you want to protect is registered to the default domain (root), proceed to Create an Encryption Key. If you need to change to a different domain, do the following:

   a. In the top menu bar, click the user name **root/admin** on the right-hand side.

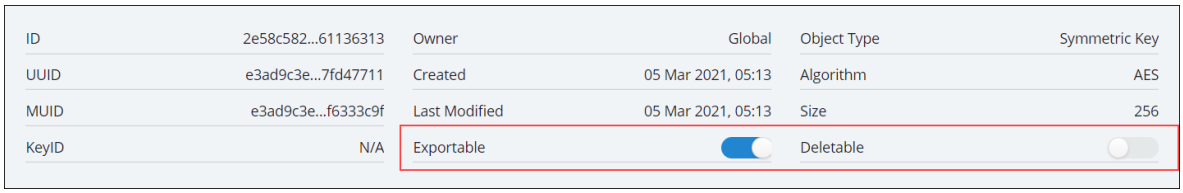
   b. Select **Switch Domains**, then select the domain in which the client is registered.

   c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

1. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.
2. Above the Key table, click **Add Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Usage** section, make sure **Encrypt**and **Decrypt** are selected.
5. Click **Add Key**. CipherTrust Manager displays the properties for the new key.
6. In the general options area, enable the **Exportable** option.
   You can also enable the **Deletable** option in this section if you want a CipherTrust Manager Administrator to be able to delete the key.

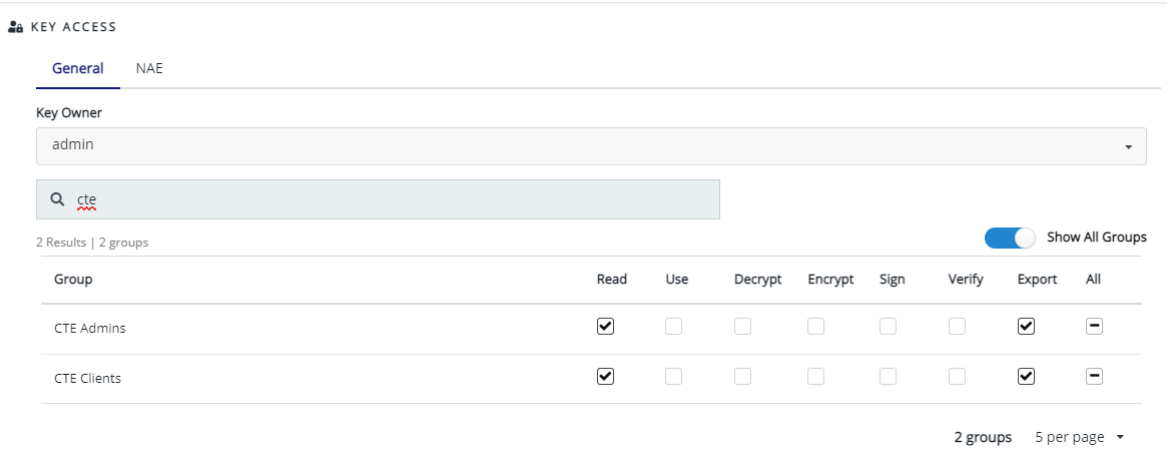


7. In the **Key Access** section, do the following:

   a. In the Search Groups box, type **CTE**.

   If no groups display, make sure that the **Added Only** option is **disabled**.

   b. Click the **Read** and **Export** option for both the CTE Admins and CTE Clients groups.



   c. When you are done, click **Update**.

8. Click the **CTE** tab and set the following properties:

   - **CTE Versioned**: Specify whether the key is versioned.

     For a standard policy, and for CTE UserSpace, you should clear this check box. If you do not, the key will not appear in the keys list when you add the key rule to the standard policy.

> **Note**
>
> CTE UserSpace **only** supports standard and offline policies. It **does not** support LDT.

   - **Persistent on Client**: Specify whether the key is stored in persistent memory on the client.

     - **Unselected**

       The keys are only stored on the disk inside the CipherTrust Manager. When required, they are downloaded to CipherTrust Transparent Encryption, but only cached in kernel memory and while encrypted. This is the default mode. The

Agent continues to work even if communication to CipherTrust Manager is not active. Note that this mode requires a stable connection between CipherTrust Manager and the CipherTrust Transparent Encryption agent in case the agent is restarted, or the server is rebooted to retrieve the keys and polices from CM.

- **Selected**

  In this mode, the keys are further encrypted with a derived key generated using a FIPS-approved derivation function and stored in the local protected directory which can be accessed only by CTE services and utilities. If the connection between CipherTrust Manager and CTE agent is not available, keys are recovered for service through the challenge/response mechanism.

- **Encryption Mode**: Encryption mode of the key:
  - **CBC-CS1**

> **Note**
>
> a. CTE-U 10.x supports **only** CBC-CS1 for new GuardPoints/deployments. Using a CBC key for a new GuardPoint can lead to data corruption.
>
> b. CTE-U 10.x is compatible with CTE-U 8.x, 9.x and ProtectFile Linux. For GuardPoints migrated from previous versions of CTE-U, and ProtectFile Linux, you can use CBC keys.

9. When you are done, click **Update**.

   For creating keys through the API, see Creating Keys for more information.

Migrating an Encryption Key

When a key is backed up and restored to a different domain or CipherTrust Manager, the KeyID may be changed. This triggers a protection code that is designed to prevent accidental use of the wrong key or double encryption. If the KeyID changes, but the key (material) is not changed, then you may see the following error when accessing a file, after the new key is pushed to the agent:

```
root@u20dev: /data-xfs/gp1# cat profile
cat: profile: Input/output error
```

Additionally, the following messages is logged in syslog:

```
    Nov  8 11:06:02 u20dev secfs_fuse[242513]: [3378] <2> [lo_open]
[fuse_check_keyid]: keyid MISMATCH (profile) inode keyid da62b804
header keyid 942ca39
    Nov  8 11:06:02 u20dev secfs_fuse[242513]: [3378] <2> [lo_open]
[fuseCTEHdr_LoadFromFD]: bad keyid check for profile (-22)
```

Since the KeyID changed, you must update the metadata stored with each file.

> **Note**
>
> Only perform the following steps if there was some sort of key migration or restoration that occurred on the CipherTrust Manager that would have resulted in the KeyID change. Accidental use of a policy with the wrong key can also result in the same behavior and messages.

To update the metadata:

1. Update the GuardPoint path. Type:

   ```
   voradmin secfs config update_keyid 1 <gp_path>
   ```

2. Restart CTE services. Type:

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

   After restart, the GuardPoint is fully accessible and the errors should no longer appear.

3. Ensure that all files in the GuardPoint are updated to the new keyid. This command does not re-encrypt any data.

   ```
   dataxform --gp <gp_path> --update_keyid
   ```

   > **Note**
   >
   > You can update the key simultaneously, while applications are accessing the GuardPoint.

4. Reset the GuardPoint back to enforcing mode to prevent accidental use of wrong key.

```
voradmin secfs config update_keyid 0 <gp_path>
```

> **Note**
>
> This does not take effect until the next restart of CTE-U, but the restart does not need to be done immediately.

5. Restart CTE services. Type:

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

Guarding CTE files with CTE-U

CTE-U can read and write CTE files encrypted with a `CS1` key on a local drive, (XFS or EXT 4). The kernel files contain a CTE header that is already compatible with CTE-U, however, that header is stored as an extended attribute on the file, and not as an embedded header.

Local file systems in CTE with CS1 keys also store header information in an extended attribute. When opening the file, if CTE-U does not find an embedded header, it looks for the existence of a header in the extended attributes.

> **Note**
>
> Thales recommends that you perform a backup in CTE and restore the backup to CTE-U. In CTE to CTE-U migration, in your policy, you **must** have full write permissions (permit, audit, all_ops, applykey) on the files copied from the CTE backup to the CTE-U GuardPoint.

Using Data Transformation to convert file headers

Data Transformation can convert the header files in the CTE from extended attribute files to embedded header files.

To convert the files, after applying your Data Transformation production policy to your GuardPoint, run the following command:

```
dataxform --scan --embed --gp <GP>
```

This forces the conversion of all file sizes so they display correctly.

See Rekeying with Data Transformation for more information.

Exporting GuardPoints over NFS

Warning

- CTE-U cannot guard a sub-directory of an exported NFS share directory. The guarded path **must** be the same as the NFS exported path.
- Use of process sets or signature sets is **not supported**.

Note

- For CTE-U v10.3.0 and subsequent versions, user sets **are supported**. See Creating User Sets for more information.

To setup and configure your NFS server so that you can export GuardPoints:

1. Make sure that CTE-U is started before the NFS server is started:

   ```
   vi /usr/lib/systemd/system/nfs-server.service
   ```

   Response

   ```
   network-online.target local-fs.target secfs-fuse.service
   ```

2. Create your GuardPoints on your NFS server.

3. Verify that the `/etc/exports` file contains the following:

```
/guardpoint/path <nfs_server_IP>(rw,sync,fsid=3,no_root_squash)
```

4. Verify that `secfs_fuse` was started before NFSD:

```
ps -ef |grep secfs; ps -ef |grep nfsd nfsd pid
```

> **Note**
>
> The GuardPoint PID is valid as long as the NFS daemon is not restarted.

5. If `secfs_fuse` was not started before NFSD, or if you are unable to verify it, restart the NFS server:

```
# service nfs-server restart
```

6. Mount the client:

```
mount -o lookupcache=none
```

> **Note**
>
> When mounting as a non-root user with NFS mount (guarded in NFS server):
>
> - Specify only the GID for the non-root user in the user set configuration in the policy.
> - Alternatively, include the root user as part of the user set configuration in the policy, but limit root user permissions. The following allows the root user to mount NFS, but they cannot read the actual data.
>   - **Action** = d_rd-att
>   - **Effect** = permit,audit

Migrating CTE Agents to CTE-U

When you have a CTE agent that is already registered with CipherTrust Manager, and you want to change it from CTE to CTE-U, you **must** perform the following steps in order:

1. Unenroll the client
2. Delete the entry from CipherTrust Manager
3. Add the client back into CipherTrust Manager
4. Install and Register the new Agent

Multifactor Authentication for CTE-U

CTE-U is supporting Multifactor Authentication through integration with an MFA provider. CTE-U will continue to integrate with additional providers and release that information in the future.

> **Note**
>
> Multifactor Authentication for CTE-U Linux is only supported with CipherTrust Manager v2.16 and subsequent versions.

- Introduction to Multifactor Authentication
- Set up your account with KeyCloak
- Use Cases for Multifactor Authentication
- Exempting some users from authentication with a Whitelist
- Setting up Multifactor Authentication with a One-Time-Password
- Setting up Multifactor Authentication with an Inactivity Time Out
- Administration for Multifactor Authentication
- Troubleshooting Multifactor Authentication

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.