THALES

AIX User Guide

FOR CTE V7.6.0

CTE Agent for AIX Installation and Configuration Guide

This document covers the following information:

- Overview
- Getting Started with CTE for AIX
- Special Cases for CTE Policies
- Logs
- Enhanced Encryption Mode
- Utilities for CTE Management
- Upgrading CTE on AIX
- Uninstalling CTE from AIX

Overview

This document describes the installation and advanced configuration options for CTE for AIX, as well as detailed information about how to integrate CTE with Oracle.

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. **Notes**: • This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". • For example, the default installation directory is /opt/vormetric/DataSecurityExpert/agent/. • For example, the default installation directory is /opt/vormetric/

Term	Description
	DataSecurityExpert/agent/ for Linux and AIX, and C:\Program Files\Vormetric\DataSecurityExpert\agent\ for Windows.
CTE 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 Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.
key manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles.
host / client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.
GuardPoint	A device or directory to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.

CTE Components

The CTE solution consists of two parts:

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

  After the CTE Agent has encrypted a device on a host, that device is called a *GuardPoint*. You can use CTE 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 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.

Note

For a list of CTE versions and supported operating systems, see the CTE Compatibility Portal.

CTE Compliance with AIX Lock Semantics

CTE is compliant with AIX lock semantics. In the following cases, CTE deviates from AIX lock semantics:

- For a guarded file, an `fclear(2)` system call will block if the current process file location and specified `fclear` number of bytes overlaps an existing file lock.
- For a non-guarded file, the `fclear(2)` system call blocks only if the `fclear` number of bytes falls within the range limits of a specified file lock.

How to Protect Data with CTE

CTE 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 the key manager through a web browser. You must have administrator privileges to create policies using either key manager. The CTE Agent then implements the policies once they are pushed to the protected host.

CTE 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.

Getting Started with CTE for AIX

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

- Installation Workflow
- AIX Package Installation
- Installing CTE with No Key Manager Registration
- Configuring CTE for AIX with CipherTrust Manager

Installation Workflow

In order to install and configure CTE, you need to perform the following high-level tasks:

1. If you want to include the CTE Agent software with the AIX distribution files, see AIX Package Installation.
2. If you want to install the CTE Agent without registering with a key manager, see Installing CTE with No Key Manager Registration. However, you cannot protect any data on the host until it has been registered. See Configuring CTE for AIX with CipherTrust Manager.
3. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see: Guarding a Device with CipherTrust Manager.

Additional Considerations

The following sections describe some of the things to keep in mind when configuring CTE.

Port Selection

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.

Communication for LDT over CIFS/NFS

All nodes that intend to use **LDT over CIFS/NFS** GuardPoint must have the following ports open:

- 7024
- 7025

Note

When you are registering a CipherTrust Transparent Encryption client with CipherTrust Manager, you can manually include a destination port number, (Default: 443). If you enter a port value, using the syntax `<hostname or IP address>:<port number>` then CipherTrust Transparent Encryption **does not** perform a port scan. CipherTrust Transparent Encryption uses the port number provided to verify the target server type using a TLS operation.

If you do not enter a port number, CipherTrust Transparent Encryption performs a port scan to check which ports are listening, including port 443.

Tracking and Preventing Local User Creation

CTE audits any attempts to change user authentication files. It also allows you to prevent any change to user authentication files using the host settings `protect`. This includes, but is not limited to user creation, modification, and deletion, or to deny users.

- The `audit` setting is set to on by default. It logs access to the system credential files but does not prevent account modifications.
- The `protect` setting both audits and prevents local user account modifications. You must manually enable the `protect` setting for tracking and prevention of local user account creation.

The `protect` tag will prevent changes to the files mentioned below. In the absence of the `protect` tag in host/client settings, operations on these files are permitted. When a log entry is generated, it is tagged with an [`audit`] tag.

- `/etc/passwd`
- `/etc/group`
- `/etc/ssh/sshd_config`
- `/etc/ssh/sshrc`

> **Note**
>
> The first time you use the `protect` host setting, you must restart CTE. Subsequent files tagged with the `protect` setting do not require a restart.

Restricted Mode

> **Caution**
>
> **If you install or upgrade in restricted mode, you cannot revert to unrestricted mode without uninstalling CTE.**

You can install CTE in restricted mode. This mode prevents any user other than `root` from accessing the following directories:

- `/var/log/vormetric`
- `/opt/vormetric/DataSecurityExpert`

Restricted Mode also prevents non-root users from running the following utilities:

- `agenthealth`
- `agentinfo`
- `check_host`
- `register_host`
- `secfsd`
- `vmd`
- `vmsec`

- `voradmin`

Key Agents and Restricted Mode

- On systems where CTE is installed in restricted mode, you cannot install a key agent (pkcs11) or CipherTrust TDE Key Management.
- On systems where a key agent (pkcs11) or CipherTrust TDE are already installed, you cannot install CTE in restricted mode.

Restricted Mode Installation

To install in restricted mode, use the -r option.

```
./vee-fs-<release>-<build>-<system>.bin -r
```

For example:

```
./vee-fs-7.2.0-56-aix71.bin -r
```

Upgrade in Restricted Mode

The upgrade mode is the same as the installation mode.

AIX Package Installation

This section describes how to install AIX packages directly so that the CTE Agent installation integrates with AIX distribution software. The CTE installation `bin` files contain the native packages and are extracted by running the `bin` file with the `-e` flag.

To extract and run the .bff file on AIX:

1. Log on to the host system as root and copy or mount the installation file onto the host system.
2. Extract the package files.

```
 ./vee-fs-7.2.0-56-aix71.bin -e
Contents extracted.
# ls *bff
vee-fs-7.2.0-56-aix71.bff
```

3. Run `installp` and then follow the prompts.

```
installp -aX -d vee-fs-7.2.0-56-aix71.bff vee.fs
```

- **If you are going to register the system with a CipherTrust Manager, see** Configuring CTE for AIX with CipherTrust Manager**.**

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see CTE Components.

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

   ```
   ./vee-fs-<release>-<build>-<system>.bin
   ```

   For example:

   ```
   ./vee-fs-7.2.0-56-aix71.bin
   ```

   To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

   ```
   ./vee-fs-7.2.0-56-aix71.bin -d /home/my-cte-dir/
   ```

   Note

   If possible, Thales recommends that you use the default directory `/opt/vormetric`.

   To view all installer options, use the -h parameter. For example:

```
./vee-fs-7.2.0-56-aix71.bin -h
```

4. The Thales License Agreement displays. When prompted, type Y and press Enter to accept.
   The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

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

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>

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

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

5. Type **N** and press Enter to end the installation procedure without registering the CTE Agent with either key manager.
   When you are ready to register the CTE Agent with a key manager, see Configuring CTE for AIX with CipherTrust Manager.

Configuring CTE for AIX with CipherTrust Manager

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

The installation and configuration process when you are using CTE with a CipherTrust Manager consists of three basic steps:

1. Installation Prerequisites
   Gather the information needed for the installation and set up your network.
2. Interactive Installation and Registration AIX

Install CTE interactively on a protected host and register the protected host with CipherTrust Manager.

Silent Installation on AIX

Install CTE silently (non-interactive) on a protected host and register the protected host with CipherTrust Manager.

3. External Certificates

   Use for communication between CTE and CM. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

4. Validating CipherTrust Manager and CipherTrust Transparent Encryption with a Local CA Certificate

   Ensure that registration by the CTE agent is serviced only by the expected key manager by providing a copy of the CA certificate that will be used to authenticate the TLS communications with the key manager.

5. Guarding a Device with CipherTrust Manager

   Create as many standard GuardPoints on the client as you need

Installation Prerequisites

This section lists the tasks you must complete, and the information you must obtain, before installing CTE.

Recommendations and Considerations

- Thales recommends that you install CTE in the default location.
- Make the installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

  For example:

```
./vee-fs-7.2.0-56-aix71.bin -d /home/hello/
```

- Ensure read/write permission is granted to other users accessing your shared resource.
- P8 Hardware Encryption is supported, but there is a required fix from IBM. If the required fix is not found, the installation defaults to Software Encryption for P8.
  - AIX 7.1 requires TL level 7100-04-04 or later.
  - AIX 7.2 requires TL level 7200-01-02 or later.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the AIX system on which you plan to install CTE to the CipherTrust Manager. After the AIX system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- It must also allow for connectivity of the CipherTrust Manager to all clients where you install CTE.
- If the system is a virtual machine, the VM must be deployed and running.

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.

Installation and Registration Options

CTE provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure.

Installation Method Options

There are two methods for installing CTE on AIX platforms:

- **Typical**: Most common and recommended type of installation. Use this method for installing the CTE Agent on one host at a time. See Interactive Installation on AIX.
- **Silent**: Create pre-packaged installations by providing information and answers to a set of installation questions. Use silent installations when installing on a large number of hosts. See Silent Installation on AIX.

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware clients.

You can enable hardware association during CTE registration process. You can disable hardware association by re-running the registration program.

Interactive Installation on AIX

The AIX typical install is an interactive script that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see Silent Installation on AIX).

After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host. However, you may postpone the registration if you plan to register CTE later.

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

Before You Begin

The following prerequisites must be met for CTE/CTE-U to install and register to CipherTrust Manager properly:

- 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.

- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot install the CTE Agent without root access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

   ```
   ./vee-fs-<release>-<build>-<system>.bin
   ```

   For example:

   ```
   ./vee-fs-7.2.0-56-aix71.bin
   ```

   To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

   ```
   ./vee-fs-7.2.0-56-aix71.bin -d /home/my-cte-dir/
   ```

   Note

   If possible, Thales recommends that you use the default directory `/opt/vormetric`.

   To view all installer options, use the `-h` parameter. For example:

   ```
   ./vee-fs-7.2.0-56-aix71.bin -h
   ```

4. The Thales License Agreement displays. When prompted, type Y and press Enter to accept.
   The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

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

```
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: <Release.build-number>

In order to register with a CipherTrust 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.
   The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: *<hostName>:<port#>*
   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
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 fo
llowing list.

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

Enter a number, or type a different host name or IP address in ma
nually:
```

```
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 s
erver 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. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloned machines from accessing the key manager (for details, see Hardware Association (Cloning Prevention) Option). The default is Y (enabled):

   It is possible to associate this installation with the hardware of this machine. If selected, the agent will not contact the key manager or use any cryptographic keys if any of this machine's hardware is changed. This can be rectified by running this registration program again. Do you want to enable this functionality? (Y/N) [Y]: Y

> **Warning**
>
> **The registration token, profile name, client group name are case-sensitive. If any of these are entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page**.

9. CTE finishes the installation and registration process.

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

Installation success.
```

10. If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.
    If you are using CipherTrust Manager version 2.1 or earlier, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Silent Installation on AIX

This section describes how to perform a silent (unattended) installation of the CTE on a single host. The silent installation automates the installation process by storing the answers to installation and registration questions in a separate file that you create. You can also use the silent installation to install CTE on multiple hosts simultaneously.

The silent install method installs CTE on the host, and registers the host with the CipherTrust Manager you specify in the silent installation file.

Prerequisites

The following prerequisites must be met for CTE/CTE-U to install and register to CipherTrust Manager properly:

- 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.
- Optionally, the name of the host group you want this client to be a part of.

Procedure

1. Log on as an administrator to the host where you will install CTE.
2. Create a parameter file and store it on your system, or copy an existing file from another location. The file can contain any of the following parameters:

   SERVER_HOSTNAME

   Required if you want to register CTE with a CipherTrust Manager.

   SERVER_IP

   Alternative for hostname when registering.

   REG_TOKEN

   The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.

   HOST_PROFILE

   Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.

   TMPDIR

   Specifies a custom temporary directory that the installer can use during the installation process. If this value is omitted, the installer uses the default temporary directory.

   AGENT_HOST_NAME

   FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

   AGENT_USEIP

   Use the IP address of the protected host instead of host name. Used when hostname is not supplied.

   AGENT_HOST_PORT

   Specifies the port number for this CTE Agent to use.

   HOST_GROUP

   Specifies the optional host/client group with which this host/client will be associated.

   HOST_DESC

Specifies a description for the host. This description is displayed in the CipherTrust Manager. If an entry for this host already exists, and the host already has a description, CipherTrust Manager **does not** overwrite the existing description, even if this option is specified.

USEHWSIG

Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.

Example 1: Registering with CipherTrust Manager

The following example contains just the required information for registration with CipherTrust Manager. In this case, the client will be registered with the CipherTrust Manager using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
AGENT_HOST_NAME=10.192.80.86
```

Example 2: Registering with CipherTrust Manager

The following example specifies the required registration information, adds a host name and description, and enables hardware association. In this case, the client will be registered with the CipherTrust Manager using its host name instead of the IP address:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
AGENT_HOST_NAME=myagent.example.com
HOST_DESC="West Coast Server 12"
USEHWSIG=1
CERT_FIELD_PARAM="/C=US/ST=California/L=San Jose/O=Thales
eSecurity/OU=Vormetrics/CN=localhost/emailAddress=admin@thalegroup.com"
SUBJECT_ALT_NAME_PARAM="DNS:www.thalesgroup.com,email:admin@thale
sgroup.com"
```

1. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.
2. Run the installer using the following syntax:

```
./vee-fs-<release>-<build>-<system>.bin [-d <custom-dir>] -s <install-file>
```

where:

- `-d <custom-dir>` is an optional parameter that specifies the installation directory for CTE. If you omit this parameter, CTE is installed in `/opt/vormetric/DataSecurityExpert/agent/`.
- `-s <install-file>` indicates that you want to install silently using the installation options file `<install-file>`

For example, if the installation options file is called `/tmp/unattended.txt`, you would enter:

```
./vee-fs-7.2.0-56-aix71.bin -s /tmp/unattended.txt
```

3. Verify the installation by checking CTE processes on the host:
   - Run `vmd -v` to check the version of CTE matches that just installed.
   - Run `vmsec status` to display CTE kernel status.
   - Look at the log files in `/var/log/vormetric`, especially `install.fs.log.<date>` and `vorvmd_root.log`.
4. In CipherTrust Manager, change the client password using the manual password creation method. This password allows users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Using external certificates for communication between CTE Agent and CipherTrust Manager

Overview

CipherTrust Transparent Encryption can now use an external certificate, available at a user-defined path, to communicate with CipherTrust Manager.

Prerequisites

The external certificate must be:

- On the file system
- In PEM format

A key pair must already exist for the client:

- Must have Encryption type of either:
  - sha256WithRSAEncryption
  - ecdsa-with-SHA384
- Must be Encrypted with a pass phrase

Initial setup

1. Obtain your external CA certificate.
2. Create a certificate using the external CA certificate and key.

CipherTrust Manager Setup

To setup CipherTrust Manager to communicate through an external certificate:

1. Import the CA certificate into the CipherTrust Manager, click **CA** > **External** > **Add External CA**.

   Note

   In the Add External CA dialog, copy and paste the `<ca_certificate_name>`.pem file content from the UI page and provide a user-friendly name.

   For more information, see Using an Externally Generated Server Certificate for an Interface
2. Add the CA certificate to the list of trusted sources for the web interface, click **Admin Settings** > **Interfaces** > **web** > **Edit** > **External Trusted CAs**.
3. Restart the web server, click **Admin Settings** > **Services** > **web** > **Restart**.
4. Create a Registration Token for the CTE agent.

CTE Agent setup

1. Create a directory on the system to hold the required files, for example:
    - `/root/cert_files` (**Linux/AIX**)
    - `c:\temp\cert_files` (**Windows**)
2. Copy or create the following files in this directory:
    - **client_cert.pem**
    - **client_key.pem**
    - **passphrase** - this is currently expected as plain text
3. For **Linux/AIX** systems, to add the directory path to the environment, type:

```
$ export EXTERNAL_CERT_DIR=/root/cert_files
```

4. For **Windows** system, invoke registerhost.exe from the command line and add this argument:

```
c:\> register_host.exe -extcertdir=c:\temp\cert_files
```

5. Register the CTE client with the CM server as normal. If this is being done as part of an installation, then the above steps should be done before the installation, or, on windows, added to the registration parameters passed to the installer.

Post Registration

During registration, the certificate file is uploaded to the CipherTrust Manager, and the certificate and key files are imported into the CTE pem store. The key is decoded using the provided passphrase, then re-encoded using a random key using the normal CTE key security mechanisms for TLS keys. There is no need to keep the input files after registration is successful, so for security reasons they should be removed / shredded.

Certificate Renewal

The location of the external certificate files (i.e. the `EXTERNAL_CERT_DIR` or `-extcertdir` parameters) will be recorded in the CTE agent configuration file, `agent.conf`. When the

current certificate is approaching expiration date (i.e. approx. 60 days prior to expiration) the CTE agent will look in this directory for an updated set of files.

If a new certificate file is present, then the file will be read and pushed to the CM, and if accepted, then the certificate and key will be imported into the CTE pem store, and the VMD process restarted to use the new certificate.

If no new certificate is present, a WARNING level message will be written to the logs and/or uploaded to the CM as per the logging settings, and the CTE agent will check again after 24 hours.

If the user wishes to change the directory path to store the new certificates, then the entry in the `agent.conf` file should be updated and the vmd service restarted. Alternatively, the user can update the external certificate set using the following command (this will not update the saved path):

```
# vmutil -a vmd -d <ext_cert_Dir> updatecerts
```

If the user fails to update the certificate set prior to expiration then communication with the CM may be blocked, and re-registration will be required.

Note

Any renewed certificates must have exactly the same common name field as the original certificate, or the CipherTrust Manager will reject the update.

Validating CM and CTE with a Local CA Certificate

To ensure that registration by the CTE agent is serviced only by the expected key manager, you can provide a copy of the root CA certificate that will be used to authenticate the TLS communications with the key manager, during the registration process.

Note

You can only download the CA certificate when you are a root user in the root domain. You cannot download the certificate from a subdomain. It will not work.

Prerequisite

Make sure that you have previously created the client in CipherTrust Manager.

Using a Local CA Certificate

1. Extract the root CA certificate from the CipherTrust Manager.
    a. Log on to CipherTrust Manager as an administrator.
    b. In the left navigation pane, click **CA > Local**. The list of available CAs displays.
    c. Click the ellipsis icon corresponding to the CA.
    d. Click **Download** to download the CA.
    e. Copy the certificate to a directory on the agent system.
2. Present the root certificate data to CTE in one of two ways:
    a. Use a file:
    When written to a file, it must be in PEM file format, starting and ending with:

    ```
    -----BEGIN CERTIFICATE-----
    -----END CERTIFICATE-------
    ```

    b. Use a a string parameter:
    If you are providing the information in a single string, it must contain the same data as in the preceding case, except that all new lines are replaced by `\n` escape sequences. For example:

    CA_CERT=-----BEGIN CERTIFICATE-----\n -----END CERTIFICATE-----\n

3. To install the root certificate into the CTE client:

```
    /opt/vormetric/DataSecurityExpert/agent/vmd/bin/
register_host.exe -s <Path-to-install-file> AGENT_HOST_NAME=<Host
name-or-IP-of-agent> REG_TOKEN=<CM registration token> CA_FILE=<P
ath-to-root-ca-cert>
```

Example

```
    /opt/vormetric/DataSecurityExpert/agent/vmd/bin/
register_host.exe -s /opt/silent/vte_reg_log.txt AGENT_HOST_NAME=a
ni-vm-217-35190.sjcicd.com REG_TOKEN=mMEz3Y6Ob9D4L7QuvK5SOmhulRm8
DYI8odV5j3OdvuHqk6LhZqE0FeIZHILYTmDiE9 CA_FILE=/cert_files/Austin1
75.pem
```

4. Confirm in CipherTrust Manager that the client is registered and healthy.

Guarding a Device with CTE and CipherTrust Manager

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

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

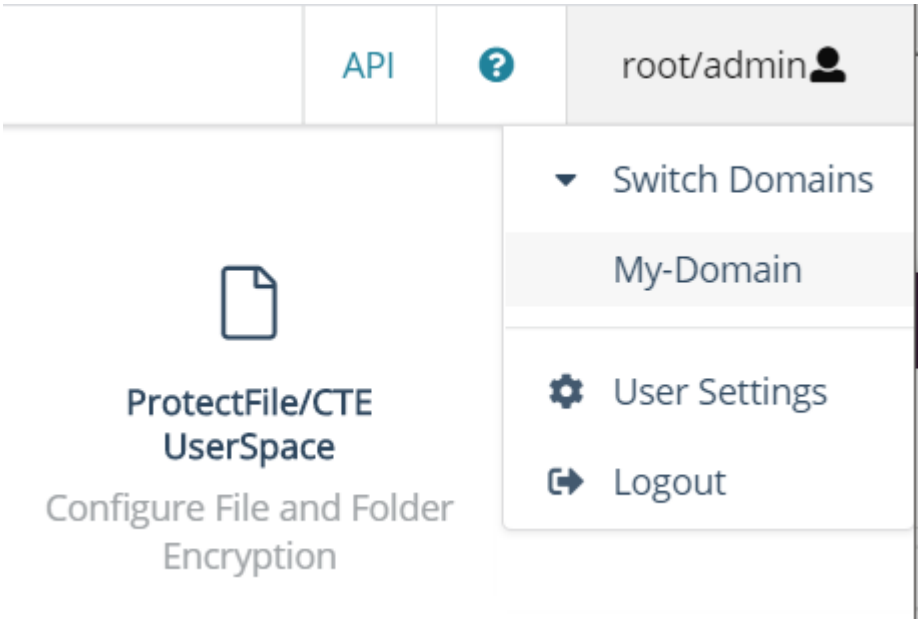
1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. Assign a GuardPoint to the device or directory.

The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

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

Note

The following procedure is based on CipherTrust Manager version 2.2. If you are using a different version, see the CipherTrust Manager documentation for the version that you are using.

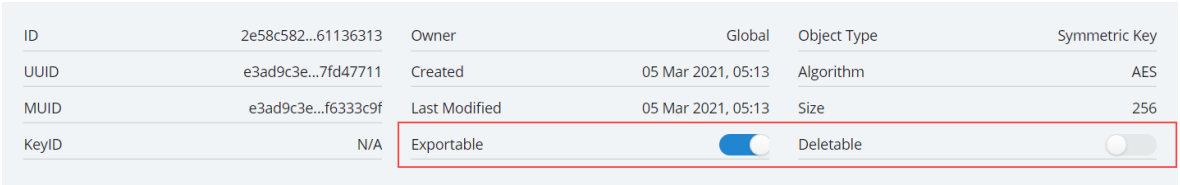
1. From the Products page in the CipherTrust Manager Console, click **Keys** in the left hand pane.

   Tip

   To navigate to the Products page from anywhere in the CipherTrust Manager Console, click the App Switcher icon in the top left corner.

2. Above the Key table, click **Create a New 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 **Create**. 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.

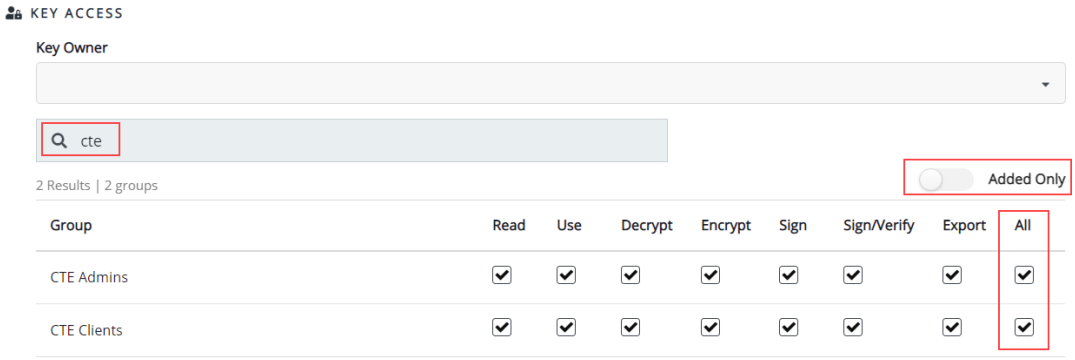


7. In the **Key Access** section, do the following:

   a. In the Search Groups box, type "cte".

   If no groups are displayed, make sure the **Added Only** option is *disabled*.

   b. Click the **All** check box 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. By default, the key is set as versioned.

     For a standard policy, 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.
   - **Persistent on Client**: Specify whether the key is stored in persistent memory on the client.

     When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.

     When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.
   - **Encryption Mode**: Encryption mode of the key. The options are:
     - CBC
     - CBC-CS1
     - XTS

     Encryption using the XTS and CBC-CS1 keys is known as enhanced encryption. For details, see the *CTE Agent for AIX Installation and Configuration Guide*.

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

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.
2. In the sidebar on the Clients page, click **Policies**.

3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.

4. On the General Info page, set the following options:

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a **Standard** policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints.
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select **Standard** as the policy type, also select the the **Data Transformation** option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

   When you are done, click **Next**.

5. On the Security Rules page, define the security rules that you want to use. CipherTrust Manager automatically adds a default security access rule with an action of `key_op` and the effects `Permit` and `Apply Key`. This rule permits key

operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version.

To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

When you are done, click **Next**.

6. On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click **Select** to choose an existing key or create a new one. If the data has not yet been encrypted, select **clear_key**. Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select **clear_key**.
Transformation Key Name	Click **Select** to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the **Current Key Name** field and re-encrypts it using the key specified in this field.

When you are done, click **Next**.

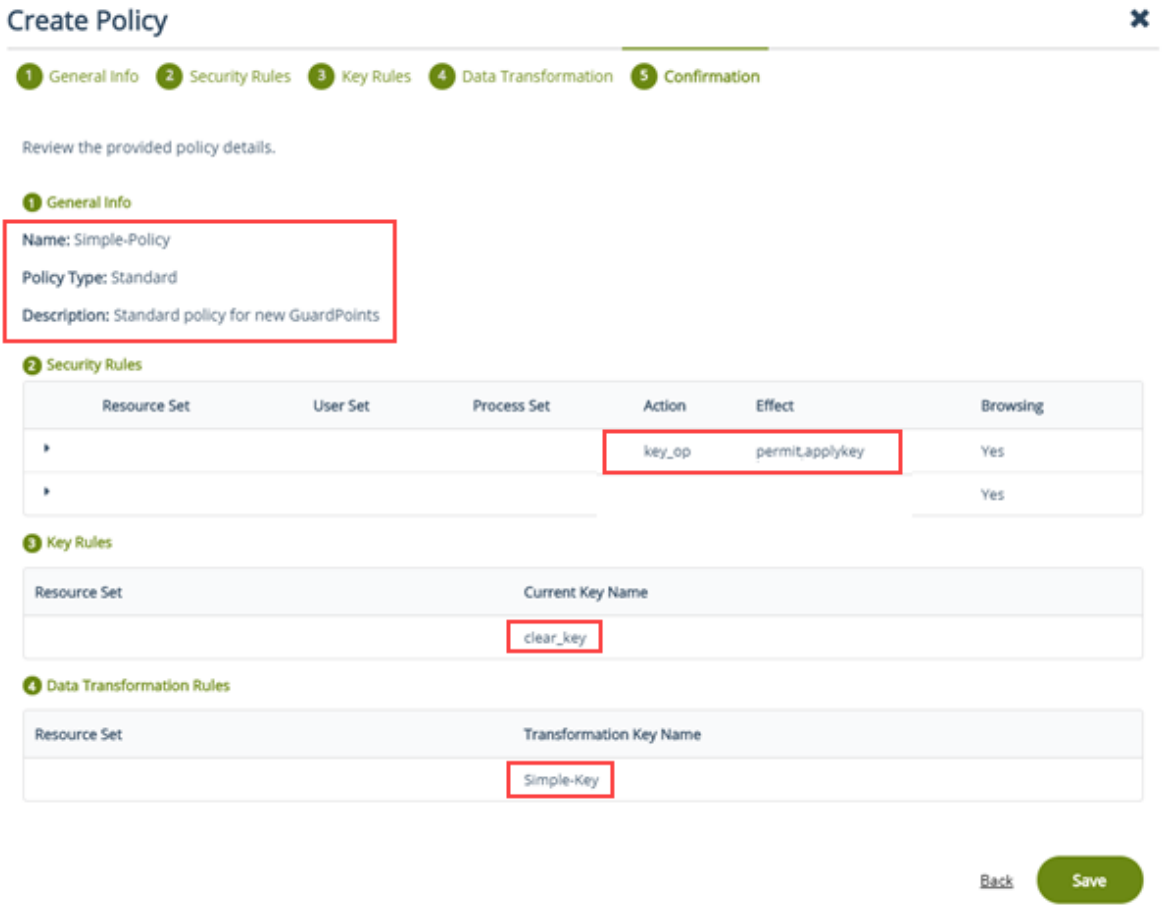
7. On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or

Field	Description
	create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click **Select** to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the **Current Key Name** field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in Create an Encryption Key.

When you are done, click **Next**.

8. Click **Next**.
9. On the confirmation page, review the information for the policy and click **Save**.



Create a GuardPoint

1. Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
2. In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
3. In the Clients table, click on the name of the client you want to protect.
4. Above the GuardPoints table, click **Create GuardPoint**.
5. In the Create GuardPoint page:
    a. In the **Policy** field, select the policy you created earlier.
    b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
    c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.
    If you want to enter multiple paths, put each path on its own line. For example:
    d. Click **Create**.
    e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

    The CTE clients pull the GuardPoint configuration information from the CipherTrust Manager.
6. Type the following to transform the data:

```
 dataxform --rekey --print_stat --preserve_modified_time --gp
<pathToGP>
```

When the data transformation has finished, applications can resume accessing the now-protected data. (See the “*CTE Data Transformation Guide*” for more information.)

Special Cases for CTE Policies

This section describes CTE-specific configuration tasks related to configuring policies in the key manager. It contains the following topics:

- Re-Enabling Automatic Signing for Host Settings
- Restricting Access Overrides from Unauthorized Identities
- Backing up DB2 Databases after Encryption
- Blocking ptrace system calls to prevent process injection attacks

Re-Enabling Automatic Signing for Host Settings

Starting with VTE for AIX release 5.2.6, VTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software that are based on the assumption that restarting the `vmd` will generate new signatures when signed software is updated. This is no longer true. However, you can re-enable automatic re-signing if your environment requires it.

Caution

Re-enabling the automatic regeneration of signatures exposes a potential security vulnerability for CTE Agents. When enabled, host setting binaries are re-signed when CTE receives a push from the associated key manager. If an attacker were to replace a binary with a Trojan, and then force a push from the key manager by, for example, restarting the CTE Agent, CTE could generate a signature for the malicious binary and pass it.

To re-enable automatic re-signing for host settings:

1. Change to the directory where the `agent.conf` file resides. For example, type:

```
cd /opt/vormetric/DataSecurityExpert/agent/vmd/etc/
```

2. Edit the `agent.conf` file.
3. Change or add the following line:

```
AUTO_RESIGN_HOST_SETTINGS=TRUE
```

> **Note**
>
> Previously this setting was known as `RE_SIGN_HOST_SETTINGS`. Starting with VTE for AIX 5.3.0, the attribute name is `AUTO_RESIGN_HOST_SETTINGS` as shown above.

4. Save your changes and exit the file.
5. Restart the `vmd` to set the changes. Type:

```
/etc/rc.d/init.d/secfs restart
```

6. Type the following command to verify that the host settings is set to true:

```
vmsec vmdconfig
```

Restricting Access Overrides from Unauthorized Identities

CipherTrust Transparent Encryption host/client settings are the means by which an administrator configures user authorization. Users with root privileges, on Linux or AIX systems, have the unfettered ability to override all file access and execution permissions imposed by the system.

CipherTrust Transparent Encryption access control allows you to restrict privileges of users, groups, application processes and binaries, including root users and setuid programs. By default, CipherTrust Transparent Encryption agent **DOES NOT** trust any process as authenticated. Any attempt to access a resource, by any process, will therefore be flagged with a “User Not Authenticated” notification. The CipherTrust Transparent Encryption agent must be instructed to trust the authenticator process progeny. For example, `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CipherTrust Transparent Encryption.

In some setups, when editing a host, system administrators can use the **host settings** > |`authenticator`| feature with `su` to change identities and gain access to restricted data. You can instruct CipherTrust Transparent Encryption to not trust any

authentication attempt performed by certain identities by assigning restricted users to a user shell that CipherTrust Transparent Encryption can block from authenticating other processes.

Any executable path that is marked with a `|path_no_trust|` host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CipherTrust Transparent Encryption prevents overrides from other host settings authenticators, using the `|path_no_trust|` status. If a user runs the `su` command from a non-trusted shell, that new shell is still marked as `|path_no_trust|`, even if `|authenticator|/usr/bin/su` is specified in the host-settings. The `|path_no_trust|` feature overrides any and all authenticators under host settings.

> **Note**
>
> Using `|trust|*` before a `|path_no_trust|` host setting no longer disables the `|path_no_trust|` host setting.

For example, the following host setting denies authentication for users accessing through sshd:

```
|trust|*
|path_no_trust|/usr/sbin/sshd
```

To restrict access overrides:

1. In the CipherTrust Manager products page, click **Transparent Encryption > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.
4. Add the following to the settings:

   ```
   |path_no_trust|<path of the binary>
   ```

   Example:

   ```
   |path_no_trust|/bin/ksh
   ```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **Apply**.

Backing up DB2 Databases after Encryption

After encrypting a DB2 database running on AIX, CipherTrust Transparent Encryption cannot make a backup of the database. Both scheduled and manual backup fail. The problem was the user's policy. An AIX policy used in this scenario must follow a few rules.

With a CBC_CS1 key, a guarded file is modified to have a 4096 byte header holding key information. When an **Apply Key** effect is specified, the CipherTrust Transparent Encryption code adjusts the length and file offset for this header. Without an **Apply Key** effect, the size and access of the offset include the CBC_CS1 header.

Thales recommends that you modify the first rule of your policy. Remove the action entry for `f_rd_att` from the first rule and add a new rule before it:

```
**action**: f_rd_att

**effect**: Permit, Apply Key
```

Policy processing starts with the first rule and continues until a matching rule is found. The effect for the matching rule is then applied.

For the `f_rd_att` action, this results in the secfs code including the CBC_CS1 key header and adjusts the file size value. Without the Apply Key effect, the file size includes the CBC_CS1 header size and the file appears as 4096 bytes larger than its real size.

Blocking ptrace system calls to prevent process injection attacks

To prevent a process injection attack, which could lead to access to encrypted data by a tampered process, Thales implemented a global blocking for the ptrace system call. The purpose of this feature is to provide configurable options for disabling the ptrace system call based on user need. CTE provides toggle options on CipherTrust Manager based on the dynamic parameter which allows a security administrator to select which binaries are protected from ptrace attachment.

> **Note**
>
> This change can be very invasive and block legitimate uses of the ptrace system call.

Options

There are three new options:

Enabled_For_Authenticators

The CTE binaries and the binaries specified in the authenticator list are protected from the ptrace attachment. Other binaries are not protected from the ptrace attachment. (Default behavior)

Enabled_For_All

All of the installed binaries are protected from ptrace attachment. This protects from a tampered processes causing process injection attacks through the ptrace attach call.

Disabled_For_All

The CTE binaries are protected from ptrace attachment but the binaries specified in the authenticator list are allowed to attach to a ptrace system call. This solves the problem of a user trying to attach a ptrace system call to one of the binaries specified in the authenticator list for other use cases. Other binaries are not protected from the ptrace attachment.

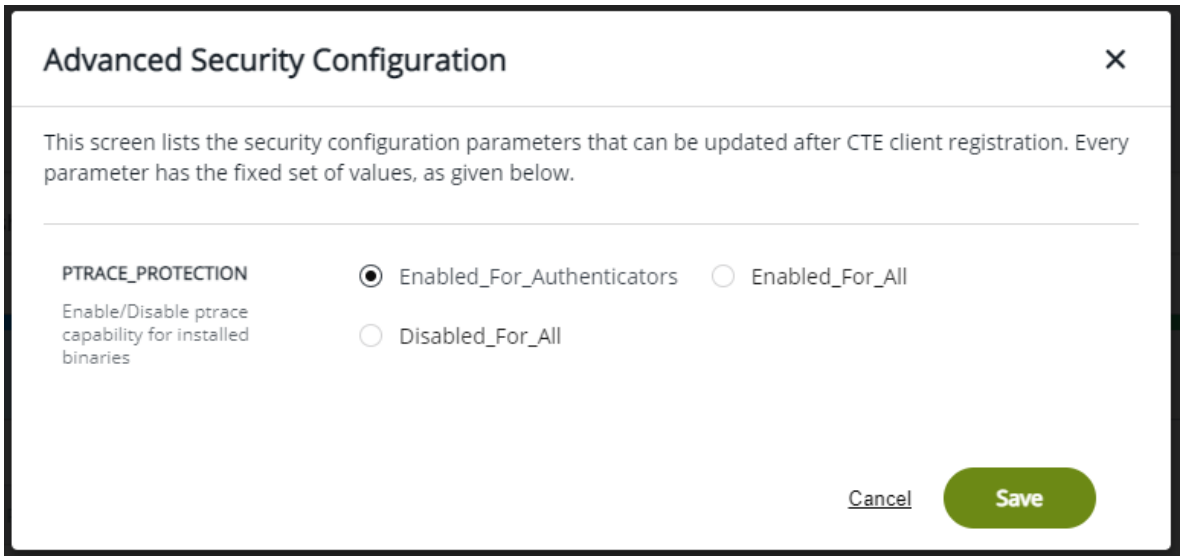
Note

If you select Disabled for All, make sure that you set the log level on CipherTrust Manager to WARN or higher. If it is set to the default log level of ERROR, there will not be any messages related to ptrace logged in the vmd.log file.

Configuration

To configure blocking the ptrace system call:

1. Log on to CipherTrust Manager.
2. Click **Transparent Encryption**.
3. Click on the desired client name to open it.
4. In the **Advanced Security Configuration**, click **View/Edit Settings** link.



5. Select the appropriate option and click **save**.

Logs

This section contains the following sections:

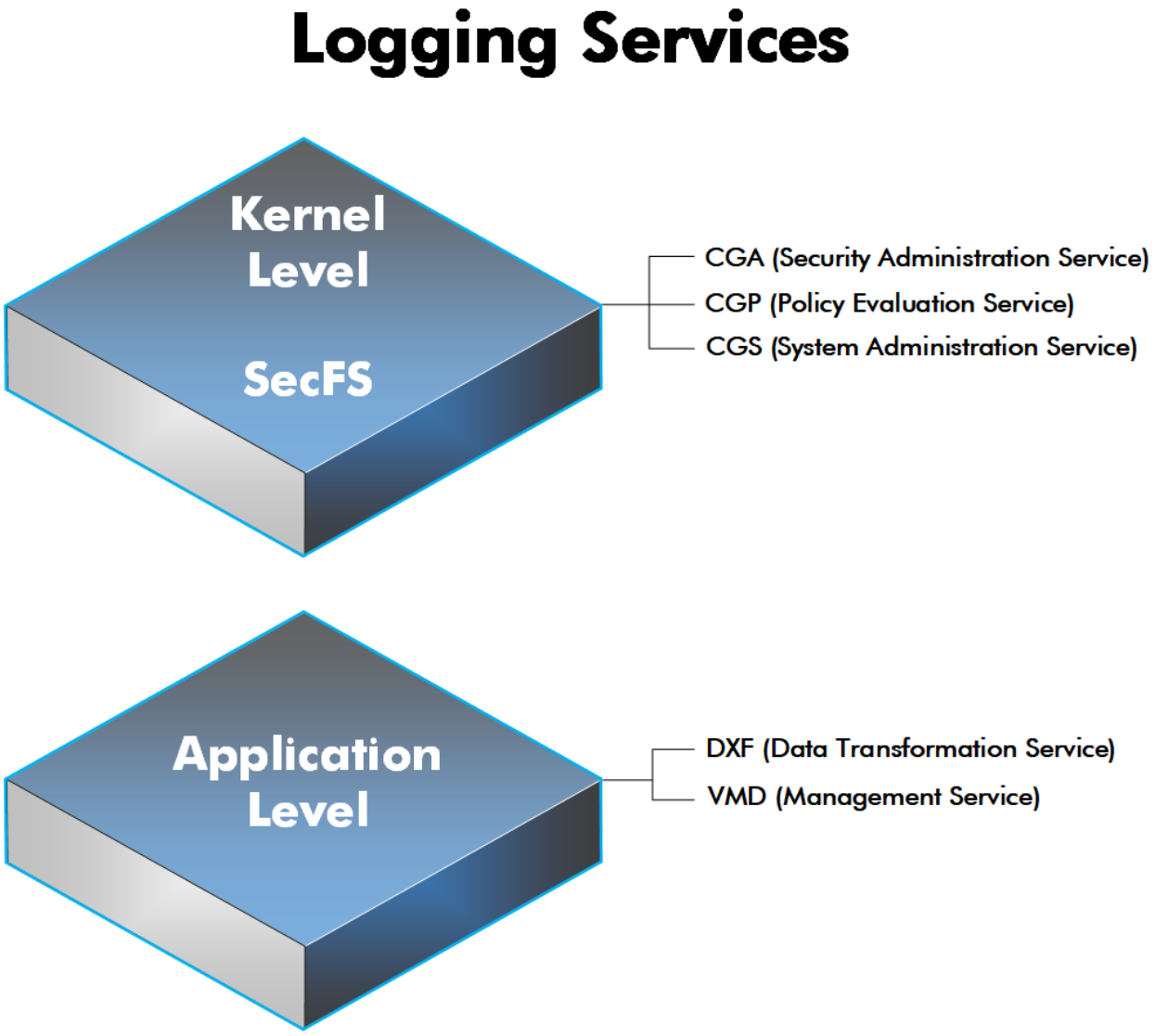
- Setting CTE Agent Logging Preferences
- Audit Logs
- Analyzing Audit log entries
- File System Audit Log Effects Codes
- Concise Logging

Setting CTE Agent Logging Preferences

You can configure the Agent process information that is entered into the Message Log. You can configure the process information globally, in which all the Agents that are added after the configuration change inherit the log attributes, while all current file system configurations remain intact. Alternatively, you can configure log attributes for individual Agent installations.

Always monitor log generation on new server and agent installations, and after changing logging preferences and options.

A variety of logging services are available and configured in the Log tab.



CTE log data may be sent to various different files such as:

- Sys log files, such as:

```
/var/log/messages

/var/log/syslog
```

Event log on

> **Note**
>
> The CM domain name can include spaces. However, Syslog does not allow spaces in header fields. Therefore, for Syslog purposes, the CTE client replaces the spaces with an underscore. For example: My_Domain instead of My Domain.

- CTE log files local to the agent, such as:

```
/var/log/vormetric/vorvmd_root.log

C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\vorvmd.log
(Windows)
```

- Uploaded to the Key Manager
- Uploaded to a Syslog server

Data Transformation log files are sent to:

```
/var/log/vormetric/vordxf_path_usr.log
```

Audit Logs

```
Example audit log:
CGP2601I: [SecFS, 0] [AUDIT] Policy[allowAllOps_fs]
User[root,uid=0,gid=0\root,bin,daemon,sys,adm,disk,wheel\] Process[/
bin/cat] Action[write_app] Res[/opt/apps/apps1/doc/file2.txt]
Key[aes128] Effect[PERMIT Code (1U,2U,3R,4M)]
```

Analyzing Audit log entries

The format of a File System Audit log entry is:

```
CGP2602I: [SecFS, 0] Level: Policy[policyName?] User[userID?]
Process[command?] Access[whatIsItDoing?] Res[whatIsItDoingItTo?]
Effect[allowOrDeny? Code (whatMatched?)]
```

Parameter	Description
Identifier	The TLA for the error message.
SECFS	Indicates that the message was generated by an Agent. You can enter `secfs` in the Search Message field in the Logs window to display the Agent policy evaluation and GuardPoint activity for all configured hosts.
Level	Indicates the importance of the message. For example, AUDIT indicates an informational message, whereas ALARM indicates a critical failure that you should not ignore.
Policy	Indicates the name of the policy that is being used to evaluate the access attempt.
User	Identifies the system user attempting to access data in the GuardPoint. It typically displays the user name, user ID, and group ID.
Process	Indicates the command, script, or utility being executed.
Access	Indicates what access is being attempted. Access may be read_dir, remove_file, write_file_attr, write_app, create_file, etc. These correspond to the Access methods that you configure in the policy. Read_dir corresponds to d_rd. Remove_file corresponds to f_rm, etc.
Res	Indicates the object/resource being accessed by the Process[].
Effect	Indicates the rule that matched and, based upon that rule, whether or not theCipherTrust Manager grants access. Access states may be either PERMIT or DENIED.

File System Audit Log Effects Codes

Codes are provided in the audit logs that identify actions by the policy enforcement engine. The code follows the number of the rule being processed.

Code	Definition
A	The Action component of a security rule failed to match.
M	All security rule components match and, unless overridden, the Effect for that security rule is applied.
P	The Process component of a security rule failed to match.
R	The Resource component of a security rule failed to match.
T	The time specified in the When component of a security rule failed to match.
U	The User component of a security rule failed to match.

Refer to the audit log example above:

- The first and second Security Rules fail because of a mismatch in the User component (1U, 2U).
- The third Security Rule fails because of a Resource component (3R) mismatch.
- All of the rules in the fourth Security Rule match (4M), and the actions defined in the policy, such as use an encryption key, are applied.

Concise Logging

Thales's standard operational logging sends audit messages for each file system operation each time a file is opened, read, updated, or written. Thales's standard logging can generate high volumes of log data. Most of these messages might not be useful or required by security administrators to monitor file system activity on the system.

Agent log data can be stored on the local host, sent to a syslog server, or uploaded to the Management Console. On an agent system, log entries can flood the local messages file or Event Log. Extreme logging can also affect network performance.

Concise Logging eliminates the following types of messages:

- Duplicate audit messages for each and every block read by the user or application. With Concise Logging, CTE only sends an audit message the *first* time a user or application performs a read/write activity. Subsequent read/write activity by that user or application is not logged.
- Audit messages that read the attributes, read the basic information of file-set attributes, and other event-based messages.
- Audit messages for directory open, read directory attributes, and directory close.

Using Concise Logging

You can enable and disable the Concise Logging option from the CipherTrust Manager for the following:

- All registered hosts in all domains
- A host that has registered with the CipherTrust Manager.

Considerations

- Concise Logging changes the set of log messages that are sent to Security Information and Event Management (SIEM) software systems. If this results in loss of data required for customer reports, then disable Concise Logging.
- Concise Logging is only supported by CTE `secfs`.
- Enable and disable Concise Logging on the client, in the Client Profile. CTE applies it for all users of that Client Profile. There is no finer-grained control, such as per GuardPoint, user, or message type.
- Do not use Learn mode with Concise Logging.

Configuring Concise Logging for CTE Clients or Client Groups with CipherTrust Manager

In CipherTrust Manager, when you create a Client Profile, you can select to Enable Concise Logging. Then, you can apply that Client Profile to a specific client, or to all clients in a Client Group. To enable Concise Logging, see the chapter *Managing Profiles in the CTE Administrator Guide*.

Enhanced Encryption Mode

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

- Compatibility
- Disk Space
- Encryption Migration
- File Systems Compatibility
- Using the AES-CBC-CS1 Encryption Mode in CM
- Exceptions and Caveats

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

> **Note**
>
> AES-CBC-CS1 encryption does not require any additional license.

Security Improvements

	AES-CBC	AES-CBC-CS1
Unique IV per-file	No	Yes
IV predictability	Yes	No

File System Support

	AES-CBC	AES-CBC-CS1
Local FS (AIX)	JFS2	JFS2
Remote FS (AIX)	NFS3/NFS4	NFS3/NFS4
Block Device Support (secvm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the CipherTrust Manager, and an error message displays.

Compatibility

- Starting with VTE for AIX version 5.3, CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- Starting with VTE for AIX version 5.3, CTE fully supports AES-CBC-CS1 encryption for offline data transformation on CTE AIX environments.

  Versions of VTE prior to version 5.3 are not backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.
- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

  Note

  - If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the CipherTrust Manager, similar to: Raw or Block Device (Manual and Auto Guard) GuardPoints are incompatible with Policy “policy-xxx" that contains a key that uses the CBC-CS1 encryption mode.”
  - AES-CBC-CS1 encryption is supported in AIX environments; as long as it is a local JFS2 or remote file system using NFS, the file formats will be compatible. It is possible that an encrypted file created with a specific AES-CBC-CS1 key on AIX cannot be read on a Linux or Windows local file system, even if that specific key were to be used, and vice versa.
- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
- Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.
- AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

	AES-CBC	AES-CBC-CS1
Local AIX FS	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.
Remote AIX FS	No change to file size. No extended attribute allocation	Extra 4KB allocation in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.

Encryption Migration

You can use offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa.
- Transform AES-CBC-CS1 encrypted data to clear contents and vice versa.

File Systems Compatibility

On AIX, you can use AES-CBC-CS1 keys to guard currently supported file systems.

AES-CBC-CS1 encrypted files on AIX local file systems can result in additional space consumption.

AES-CBC-CS1 files on AIX local or remote file systems such as JFS2 embed the IV in a 4K-byte header within the file. When these files are guarded, CTE masks the file header to applications and system utilities. The expanded file is only apparent when CTE guarding is disabled.

Note

The file system must have enough extra space to store the extra 4K bytes of the embedded header.

On AIX, with AES-CBC-CS1 encryption, encrypted files on all file systems, both remote or local, have the same file format.

Storing Metadata

AES-CBC-CS1 encrypted files on AIX store the base IV of a file in the embedded header of the file.

To get the value of the base IV, type:

```
voradmin secfs iv get <file-name>
```

Note

The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

Using the AES-CBC-CS1 Encryption Mode in CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the Managing Policieschapter in the CTE Administrator Guide.

Best Practices for AES-CBC-CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC-CS1 keys unless all hosts are running VTE for AIX version 5.3 or CTE version 7.0.0 or later.

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Guarding Existing Files Without Data Transformation

You must convert an existing file with clear text through offline data transformation. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Best Practices for AES-CBC CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC CS1 keys unless all hosts are running VTE for AIX version 5.3 or CTE version 7.0.0 or later.

Utilities for CTE Management

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

- Agent Health Return Codes
- Agentinfo (Java version)
- Backup
- Check_host
- Displaying Information for Nested File Systems with the DF tool
- Protecting Files with Client Settings
- Restricting Access Overrides with Client Settings
- Register_host
- SecFSD
- Using Client Settings with Shell Scripts
- Vmutil

- VMsec
- VMD

Agent Health Utility

The `agenthealth` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to CipherTrust Manager Server
- CTE processes/ modules that are running
- Available disk resources
- Current GuardPoints
- Tests if the agent can reach the GuardPoints
- CTE log directory resource status
- This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain vmd/SecFS information. They are regenerated whenever secfs restarts. If the number of files is unexpectedly large, this can indicate a problem.

The Agent Health check script

By default, the `agenthealth` script is installed in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`.

To run the `agenthealth` check script, type:

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
```

System Response

```
Checking for super-user privilege ..............  OK
CipherTrust Agent installation ..................  OK
CipherTrust policy directory ....................  OK
Registration to server ..........................  OK
Kernel modules are loaded .......................  OK
VMD is running ..................................  OK
SECFSD is running ...............................  OK
```

```
dsm4209.sjinternal.com is resolvable ..... OK
dsm4209.sjinternal.com port 8446 is reachable .... OK
dsm4209.sjinternal.com port 8447 is reachable .... OK
Can communicate to at least one server ..... OK
VMD is listening on port 7024 ..... OK
Time of last update from server ..... 2021-07-07
15:47:08.290
Checking available disk space ..... OK
Checking logging space ..... OK
        Log directory is "/var/log/vormetric"
        File system for log data is "/", 48G free (5% full)
        Log directory contains 9 of maximum 200 files (4% full)
        Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to /media ..... OK
Testing access to /usr/data/sub1 ..... OK
[root@agt4206 bin]#
```

Agent Health Return Codes

Previously, the agent health return codes were only available in `/var/log/vormetric/agenthealth.log`. Now, the following options are also available through the help pages:

Help

This agent health script checks various facets of the CipherTrust agent to make sure that everything is functioning properly. Results are also logged to `/var/log/vormetric/agenthealth.log`.

Syntax

```
./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --help
```

Return Codes

Use the return code option to get a list of the return codes and what they mean. The codes are returned if the Agent is not running.

Syntax

```
 ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth --
return_codes
```

Response

Return Code	Definition
EPERM	User is not root.
ENOENT	One of the programs used in this script does not exist. See `/var/log/vormetric/agenthealth.log` for which program is missing.
ENOPKG	Agent software is not properly installed. Agent configuration directory is missing or corrupt. See `/var/log/vormetric/agenthealth.log` for more details.
EPROTO	Agent is not registered to a key manager. Register the agent to a key manager and try again. Try the wait option if the a gent has never started correctly after registration. See `/var/log/vormetric/agenthealth.log` for more details.
EIO	Kernel modules are not loaded. To load a kernel module, type: `/etc/vormetric/secfs start`
ESRCH	VMD is not running. To start vmd manually, type: `/usr/bin/vmd`
SECFSD	Secfsd is not running. To start the secfsd manually, type `/usr/bin/secfsd`
EHOSTUNREACH	Unable to reach the Key Manager. Check network connectivity.
ECONNREFUSED	VMD is not listening. VMD did not finish initialization. See `/var/log/vormetric/vmd.log`
EWOULDBLOCK	VMD is attempting to connect to the Key Manager but has exceeded the designated wait time. Check `/var/log/vormetric/vmd.log` to fix any issues and retry.

Wait Time

Use --w to set a maximum wait time in seconds. The minimum is 10 seconds to test for the VMD to Key Manager initial contact. The default setting is 0, which means that there is no wait. Maximum is 1200 seconds.

Syntax

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/
agenthealth --w <value>
```

Example

```
[root@agt4206 bin]# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin//
agenthealth --w 60
```

Response

```
Checking for super-user privilege ..............  OK
CipherTrust Agent installation ..................  OK
CipherTrust policy directory ....................  OK
Registration to server ..........................  OK
Kernel modules are loaded .......................  OK
VMD is running ..................................  OK
SECFSD is running ...............................  OK
dsm148.i.vormetric.com is resolvable ............  OK
dsm148.i.vormetric.com port 8446 is reachable ....  OK
dsm148.i.vormetric.com port 8447 is reachable ....  OK
Can communicate to at least one server ..........  OK
VMD is listening on port 7024 ...................  OK
Time of last update from server .................. 2021-08-18
10:34:56.665
Checking available disk space ...................  OK
Checking logging space ..........................  OK
Log directory is "/var/log/vormetric"
File system for log data is "/", 29G free (23% full)
Log directory contains 1 of maximum 200 files (0% full)
Log directory contains 0 of maximum 100 Mbytes used (0% full)
```

If the customer did not use the wait time options, the output would look similar to the following:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/agenthealth
Checking for super-user privilege ..............  OK
```

```
CipherTrust Agent installation .................. OK
CipherTrust policy directory .................... OK
Registration to server .......................... OK
Kernel modules are loaded ....................... OK
VMD is running .................................. OK
SECFSD is running ............................... OK
Can communicate to at least one server ........... FAILED
For more information consult the log file /var/log/vormetric/
agenthealth.log
```

agentinfo Utility (Java version)

The `agentinfo` utility collects system and CTE configuration data. The `agentinfo` utility is used to take a configuration snapshot of the system that you will send to Thales Customer Support to debug an issue, (This section describes the Java version.)

The `agentinfo` utility is a Java Script file. You can open it in a text editor to see specific functions.

The `agentinfo` utility displays status information on the screen and outputs the results to a compressed tar file. The compressed tar file name format is `ai.<os_name_ver>.qa.com.tar.gz` and it is located in the current working directory.

To create an agentinfo file, type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/agentinfo
```

check_host Utility

If a CTE software installation fails during the certificate generation and exchange stage, use the `check_host` utility to list the network addresses for the host. The utility checks network interfaces, `/etc/hosts`, DNS, and so on, to compare, test, and evaluate possible addresses for the host, and weights them based upon their network efficiency. FQDNs are the most preferred and stand-alone IP addresses are the least preferred. Some applications, such as silent-mode installation, use `check_host` to determine the best host address to submit to the CipherTrust Manager during registration.

Run the `check_host` utility on a system that is hosting CTE to display available network host names, FQDNs, and IP numbers for the host.

Type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/check_host
```

check_host Syntax

```
check_host [[-h | -i | -a ] [-s name]] |
-l name:port[,name:port] | -r name
```

Syntax	Description
-h	Print the best host name for this machine
-i	Print the best IP address
-a	Print all the host names and IP addresses
-s	The name of the server (optional hint)
-r	The name of the server for name resolution checks
-l	The name and port of the server for listening checks

Displaying Information for Nested File Systems with the DF tool

When a file system mounts on top of another file system, the command `df -a` does not display the attributes for the covered file system.

On Linux environments, this is the expected behavior for any file system that is overlayed by another file system.

The secfs driver properly handles the call, which is made by the `statfs` system call, which is issued by the df tool. When the system call returns, its structures are correctly populated with the details of the nested file system. On examining the source of the df tool, it is found that when the `-a` switch is on, it nullifies the stats which are received for overlayed mounts. When the `-a` option is not enforced, the stats are maintained.

Issue the `df` command for a specific mount point, for example `df /xfs/nested-xfs` (where `/xfs` is a secfs GuardPoint). It works correctly.

Protecting Files with Client Settings

When any file is now marked as protected (|protect|) in the client settings, that file is protected from being modified or deleted, (even from a root process).

> **Note**
>
> The file is not guarded and it can be external to a GuardPoint.

Previously, the only files that were protected were the following:

```
/etc/passwd
/etc/group
/etc/security/passwd
/etc/ssh/sshd_config
/etc/ssh/sshrc
/opt/testfile
```

If the file marked as |protect| does not exist, then CipherTrust Transparent Encryption creates a 0-length file in its place. This provides an efficient means to identify and implement file protection. When the agent is stopped or uninstalled, these 0-length files are deleted and then re-created if the agent is restarted. Additionally, an audit record is generated when a file operation is denied.

The `|protect|` status is displayed using `secfsd -status auth.`

Restricting Access Overrides with Client Settings

CipherTrust Transparent Encryption host/client settings are the means by which an administrator configures user authorization. Users with root privileges, on Linux or AIX systems, have the unfettered ability to override all file access and execution permissions imposed by the system.

CipherTrust Transparent Encryption access control allows you to restrict privileges of users, groups, application processes and binaries, including root users and setuid programs. By default, CipherTrust Transparent Encryption agent **DOES NOT** trust any

process as authenticated. Any attempt to access a resource, by any process, will therefore be flagged with a “User Not Authenticated” notification. The CipherTrust Transparent Encryption agent must be instructed to trust the authenticator process progeny. For example, `/usr/sbin/sshd` is a process that can be trusted to authenticate the user to the system and to CipherTrust Transparent Encryption.

In some setups, when editing a host, system administrators can use the **host settings** > |`authenticator`| feature with `su` to change identities and gain access to restricted data. You can instruct CipherTrust Transparent Encryption to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CipherTrust Transparent Encryption can block from authenticating other processes.

Any executable path that is marked with a |`path_no_trust`| host setting marks the process, and all child processes, as not trusted. Non-trusted processes are treated as "User Not Authenticated" to prevent access on user-based policies.

CipherTrust Transparent Encryption prevents overrides from other host settings authenticators, using the |`path_no_trust`| status. If a user runs the `su` command from a non-trusted shell, that new shell is still marked as |`path_no_trust`|, even if |`authenticator|/usr/bin/su` is specified in the host-settings. The |`path_no_trust`| feature overrides any and all authenticators under host settings.

Note

Using `|trust|*` before a `|path_no_trust|` host setting no longer disables the `|path_no_trust|` host setting.

For example, the following host setting denies authentication for users accessing through sshd:

```
|trust|*
|path_no_trust|/usr/sbin/sshd
```

To restrict access overrides:

1. In the CipherTrust Manager products page, click **Transparent Encryption > Clients**.
2. Click on an existing Client name to edit the host.
3. Click **Client Settings** tab.

4. Add the following to the settings:

```
|path_no_trust|<path of the binary>
```

Example:

```
|path_no_trust|/bin/ksh
```

The above example indicates that no process under the kshell executable will be authenticated.

5. Click **Apply**.

register_host Utility

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, and to register CTE on the CipherTrust Manager. After the host is registered, you can configure CTE, apply GuardPoints, or perform database backups. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

secfsd Utility

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

- GuardPoints defined in the *GuardPoints* tab
- Authentication parameters defined in the *Host 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 `secfs` utility is also used to mount GuardPoints for `Directory (Manual Guard)`. Normally, CTE automatically mounts the `secfs` file system when you apply a GuardPoint to a directory. On AIX, 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 keys`	show current encryption key state
`-status auth`	list authentication settings
`-status lockstat`	show CTE lock status
`-status logger`	list logging details
`-status policy`	list configured policies
`-status pslist`	list protected processes
`-status devmap`	list guarded devices

Manual GuardPoint options

Command	Description
`-guard path [container ID]`	manually guard path
`-unguard path [container ID]`	manually unguard path

Version option

Command	Description
`-version`	list version of kernel module `secfs2`

Encryption Mode option information

Command	Description
`crypto`	Displays the encryption modes that are supported.

Configuration Mode option information

Command	Description
`config <config_param> <value>`	Displays the encryption modes that are supported.

secfsd Examples

- Display GuardPoint Information
- Display GuardPoint Information in a Different Format
- Display Host Settings
- Display Key Status
- Display Lock Status
- Agent Security Configuration Protection
- Display CTE Log Status
- Display Applied Policies
- Display CTE Process Information
- Display CTE Version Information
- Manually Enable a GuardPoint in CipherTrust Manager

Display GuardPoint Information

To display the GuardPoint paths, applied policies, policy type, and guard status, use the `secfsd -status guard` command. For example:

```
secfsd -status guard

GuardPoint    Policy           Type             ConfigState
Status        Reason
----------    ----------       -----            -----------
------        -----
/opt/apl/lib  allow AllOps_fs  local            guarded
guarded       N/A
/dev/sdb      watchaccess_rd   rawdevice        guarded
guarded       N/A
/dev/sdc      watchaccess_rd   manualrawdevice  guarded
```

```
guarded      N/A
/dev/sdd     watchaccess_rd   manualrawdevice  unguarded     not
guarded  Inactive
/opt/apl/tmp MSSQL00123       manual           unguarded     not
guarded  Inactive
```

Column	Description
GuardPoint	Full path of the GuardPoint.
Policy	Name of the policy applied to the GuardPoint.
Type	Can be local, automount, manual, raw device, or manual raw device. Configured in the **GuardPoints** tab.
ConfigState	Guard status of the GuardPoint, as recognized by the key manager. It can be guarded or unguarded.
Status	Current guard status, as recognized by CTE. State can vary.
Reason	Additional information about the status, if any.

Note

- Config State and Status can vary. As an example, if you apply a GuardPoint and someone is currently working in the GuardPoint, the policy cannot be applied at that time. In this case, the ConfigState is guarded and the Status is not guarded.
- When the user removes an auto-mounted GuardPoint from CipherTrust Manager, the CTE Agent is only deleted after the configured `autofs` timeout expires. This timeout does not start until the GuardPoint is free.

Display GuardPoint Information in a Different Format

To display the same information in a block format, use the `secfsd -status guard -v` command. For example:

```
secfsd -status guard -v

GuardPoint: 1
```

```
        Policy:          allowAllOps_fs
        Directory:       /opt/apps/apps1/tmp
        Type:            local
        ConfigState:     guarded
        Status:          guarded
        Reason:          N/A
GuardPoint: 2
        Policy:          allowAllRootUsers_fs
        Directory:       /opt/apps/apps1/lib
        Type:            local
        ConfigState:     guarded
        Status:          guarded
        Reason:          N/A
```

Display Host Settings

To display the SHA2 hash signature for each protected host setting, use the `secfsd -status auth` command. For example:

```
secfsd -status auth

|authenticator|/bin/su
3E765375897E04C39AB17D4C755F50A35195535B6747DBA28DF9BD4AA672DFF9
|authenticator|/usr/sbin/sshd
98FC599D459EDEA52A60AB394B394803B5DAB96B53148DC608732DDA6777FA1A
|authenticator|/usr/sbin/in.rlogind
5C9A0EDD8BF54AE513F039476D21B3032507CF957AA0CB28C368EB8AB6E684FB
|authenticator|/bin/login
0D2EE0B995A30AE382B4B1CA5104715FC8902F457D283BDABAAD857B09259956
|authenticator|/usr/bin/gdm-binary
363780522E3CCF9ABF559F059E437743F9F97BBBB0EE85769007A464AD696BD1
|authenticator|/usr/bin/kdm
BAD41BBCDD2787C7A33B5144F12ACF7ABC8AAA15DA9FDC09ECF9353BFCE614B5
```

Display Key Status

To display the status of CTE keys, use the `secfsd -status keys` command. For example:

```
secfsd -status keys
Encryption keys are available
```

Display Lock Status

To display the status of CTE locks, use the `secfsd -status lockstat` command. For example:

```
secfsd -status lockstat
FS Agent Lock: false
System Lock: false
```

The value is **true** if the lock is applied. The value is **false** if the lock is not applied. **System Lock** corresponds to **System Locked** in the *Host* window. **FS Agent Lock** corresponds to **FS Agent Locked** in the *Host* window.

Note

Before you upgrade, remove CTE software, or change operating system files, the status of FS Agent Lock and System Lock must be false.

Agent Security Configuration Protection

The Agent lock directory, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec` contains secfs secret files, configuration files, host setting signatures, etc. Thales recommends protecting the directory whenever secfs is online.

Applying improved directory protection ensures that only CTE applications (`vmd, secfsd, voradmin`, etc.) can modify the .sec directory and the files in it. All users, including root, are denied read/write access to the files. They also do not have permissions to modify `conf` and `bin` directories, using other tools.

A new command has been created to protect the directory: `voradmin secfs config`

Syntax

```
voradmin secfs config <configuration_parameter> <value>
```

Example

```
voradmin secfs config pagecache_writeback 1
```

Previously, you would have had to use the following command to achieve the same results as the example above:

```
echo 1 > /opt/vormetric/DataSecurityExpert/agent/secfs/.sec/conf/
pagecache_writeback
```

Note

When CTE is upgraded to v7.2.0 from the previous release, it may display 'Permission Denied' warnings which display when files are removed from subdirectories of the `.sec` directory. You can ignore these warnings. They are harmless.

Display CTE Log Status

To display the status of CTE log service, use the `secfsd -status logger` command. For example:

```
secfsd -status logger

Upload URL: https://vmSSA06:8444/upload/logupload,https://vmSSA07:84
44/upload/logupload, \
https://vmSSA05:8444/upload/logupload
Logger Certificate directory: /opt/vormetric/DataSecurityExpert/age
nt/vmd/pem
```

This command sequence returns the URL to which the log service sends log data. It also returns the directory that contains the CTE certificate. CTE uses the certificate to authenticate CTE when it uploads the log data to the CipherTrust Manager.

Display Applied Policies

To display the policies that are applied to CTE, use the `secfsd -status policy` command. For example:

```
secfsd -status policy

Policy: enc-audit
Type: ONLINE
```

Display CTE Process Information

To display CTE processes, use the `secfsd -status pslist` command. This command shows the process number associated with each CTE process. To show the details about a specific CTE process, use the `ps -fp <process #>` command, where `<process #>` is the process number from the `secfsd -status pslist` command.

For example:

```
secfsd -status pslist
Protected pid list:     739   731

ps -fp 739
UID     PID   PPID  C   STIME      TTY  TIME   CMD
root    739   1     0   11:04:56    -   0:00 /opt/vormetric/   \
    DataSecurityExpert/agent/vmd/bin/vmd
```

Display CTE Version Information

To display CTE version information, use the `secfsd -version` command. For example:

```
secfsd -version
version: <Release.build-number>
```

Manually Enable a GuardPoint in CipherTrust Manager

To manually enable a GuardPoint on an AIX host:

1. Click **CTE > Clients> <*clientName*> GuardPoints**
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.
4. Set Type to **Manual Directory**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **Create**.
7. Log onto the system hosting CTE as the root user.
8. To manually enable the GuardPoint, use the `secfsd -guard <path>` command. For example:

```
secfsd -guard /opt/apps/etcsecfsd: Path is Guarded
```

9. To verify the change, use the `secfsd -status guard` command. For example:

```
secfsd -status guard

GuardPoint      Policy          Type    ConfigState  Status
Reason
----------      ------          ----    -----------  ------
------
/opt/apps/etc   allowAllOps_fs  manual  guarded      guarded
N/A
```

secfsd and Raw Devices

CTE only creates block devices. To display them, use the ls `-l /dev/secvm/dev` command. For example:

```
 ls -l /dev/secvm/dev

brw-------    1 root     system       38,  1 Jan 29 16:37 hdisk1
brw-------    1 root     system       38,  2 Jan 29 16:37 hdisk2
crw-------    1 root     system       38,  3 Jan 29 16:37 rhdisk1
crw-------    1 root     system       38,  4 Jan 29 16:37 rhdisk2
```

Using Client Settings with Shell Scripts

Client settings on a shell script do not work as expected in AIX. This is because a shell script is not executed as a binary by a shell, rather, it is interpreted by the shell as a sequence of commands.

This limitation may be overcome by running the shell script in the context of a binary. A program is constructed to issue an `execl(2)` of a shell with the desired script as its argument.

The client settings are then applied to the binary. When it executes, the client setting is applied to it by the agent code. Therefore, when it runs the shell, the client setting is inherited by the shell and is subsequently applied to all of the commands run as the script executes.

Following is an example program for implementing Client Settings:

```
    cc testcode.c -o testcode
    -------------------------

    #include <unistd.h>
    #include <errno.h>
    #include <stdlib.h>

    int
    main(int argc, char *argv)
    {
        int rv;

        rv = execl("/usr/bin/ksh", "ksh", "./testdata", NULL);
```

```
        if (rv < 0) {
                printf("execl errno %d\n", errno);
                exit(1);
        }

        exit(0);
    }
```

- The file, testdata, contains the shell script text.
- For test purposes, use a shell script that contains:

```
/usr/bin/cat
```

- The client setting is applied to the testcode binary. When it runs, the client settings are applied to the components of the script, testdata.

vmutil

Usage

```
vmutil <options> <operations>
```

Options

Option	Function	Description
-a	--agent	Specify agent type (vmd or pkcs11)
-d	--extdir	Specify location of external certificate and key set
-e	--error	Specify one or more errors for state report
-h	--help	Display help and exit
-l	--loglevel	Specify log output level (debug, info, warn, error or fatal)
-f	--force enabled	Force option for delete host operation
-v	--version	Display program version and exit

Operations

Operation	Description
certexpiry	Report the certificate expiration date for this agent

Operation	Description
deletehost	Delete this client from the server
renewcerts	Renew certificate set for this agent
reportstate	Report agent state and error conditions to server
unregister	Unregister this agent/client from the server
updatecerts	Update external certificate and key set for this agent/client

vmsec Utility

The vmsec utility allows you to manage security aspects of CTE on the host. On AIX hosts, the `vmsec` utility is located in:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/vmsec
```

vmsec Syntax

Syntax	Description
`checkinstall`	Show vmd kernel status
`challenge`	Enter the dynamic host password
`vmdconfig`	Display the vmd configuration
`check_hwenc`	Display kernel configuration
`hwok`	Report status of hardware signature
`passwd [-p <password>]`	Enter the static host password
`version`	Display CTE version

vmsec Examples

- Display CTE Challenge String
- Display CTE Status
- Entering a Password
- Display Kernel Status
- Display CTE Build Information
- Display Contents of Conf files

Display CTE Challenge String

To display a CTE password challenge string and enter the response string when the CipherTrust Manager is not network accessible, use the `vmsec challenge` command. This command displays a challenge string that you can send to your key manager administrator, who will then send you back the correct response information.

For example:

```
 vmsec challenge
Contact a Security Server administrator for a response.
Your hostname is host120.my.domain.com
Your challenge is: F5TL-42HU-5H6Y-EJCK
Response (part 1) -> 6B2T-Q3DV-5EK3-QOFD
Response (part 2) -> XBP5-LQXB-TDWA-SILG
Response (part 3) -> XSEA-CQB5-S6U5-3YWV
Response (part 4) -> KXRS-QYXB-BP74-C4RN
Success!
```

Contact your key manager administrator and give them the challenge string. The administrator will give you four response strings. Enter the first response string in the **Response (part 1)** field and press **Enter**, then enter the second, third, and fourth response strings in the same way. You have 15 minutes to enter the first response string.

> **Tip**
>
> If you are using CipherTrust Manager, the ability to change the contact string will be added in a future release. For CipherTrust Manager, the contact string says "Contact your CM administrator".

Display CTE Status

This utility shows you if CTE is configured and running. If it is not running, you might need to start it manually. To display CTE status, use the `vmsec checkinstall` command. For example:

```
vmsec checkinstall
The kernel component is installed and running.
```

Entering a Password

To enter the CTE static host password, use the `vmsec passwd` command. For example:

```
 vmsec passwd
Please enter password:
OK passwd
```

To enter CTE static host password on the command line so you can specify it in a batch script, specify the password using the -p option. For example:

```
 vmsec passwd -p myPass123
OK passwd
```

Display Kernel Status

To display the kernel status, use the vmsec status command. For example:

```
vmsec status
FILE_FORMAT=2
FILE_GENERATED=08/27/2019 18:54:10
SA_QOS_STATUS=0
SA_HOST_CPU_UTIL=0
GP_1_Policy=27
GP_1_Dir=/gp
GP_1_lock=1
GP_1_type=1
GP_1_gtype=manual
GP_1_opt=gtype=2,policy=27,lock=1,type=1,dir=/gp/
GP_1_config_state=unguarded
GP_1_status=not guarded
GP_1_statuschk_tm=0-00-00 00:00:00
GP_1_config_op_retry_cnt=0
GP_1_config_op_attempt_tm=0-00-00 00:00:00
GP_1_flags=0
```

```
GP_1_reason=Inactive
GP_1_usage=free
TOTAL_GP=1
KEYS_AVAILABLE=TRUE
sdk_version=<Release.build-number>
sdk_builddate=2019-08-19 15:16:46 (PDT)
coreguard_locked=false
system_locked=false
logger_upload_url=https://thl602-2114.qa.com:8447/upload/logupload,htt
ps://thl602-2116.qa.com:8447/upload/logupload
logger_cert_dir=/opt/vormetric/DataSecurityExpert/agent/vmd/pem
hostname_for_logging=vmd
QOS_PAUSED=false
vmd_STRONG_ENTROPY=false
vmd_URL=https://thl602-2114.qa.com:8446
vmd_SRV_URLS=https://thl602-2114.qa.com:8446, https://thl602-2116.qa.c
om:8446
vmd_PRIMARY_URL=https://thl602-2114.qa.com:8446
vmd_SUPPORTS_F8P=TRUE
vmd_SUPPORTS_CR256=TRUE
vmd_RANDHP=TRUE
learn_mode=false
concise_logging=false
vmd_listening_port=7024
vmd_initialization_time=2019-07-25 12:07:14.514
vmd_last_server_update_time=2019-07-25 12:12:04.747 policy_name_27=aes2
56
policy_version_27=0
policy_keyvers_27=0
policy_type_27=ONLINE
policies=27
logger_suppression_VMD=SUPPRESS
logger_intervaltime_VMD=600
logger_repeat_max_VMD=5
logger_suppression_POL=SUPPRESS
logger_intervaltime_POL=600
logger_repeat_max_POL=5
CONFIG_SA_1=27
```

```
TOTAL_CONFIG_SA=1
SA_1_NAME=27
SA_1_ALIAS=aes256
SA_1_TYPE=0
SA_1_REF=1
SA_1_HIP_REG_TIME=0
SA_1_FLAGS=1
TOTAL_SA=1
TOTAL_AUTH=0
AUTHBIN_1=|authenticator|/usr/sbin/sshd B92A3D7EEF67B82230F7F76097D6515
9FCF5722A4154A249EFDC22C20F1B572C
AUTHBIN_2=|authenticator|/bin/login 4F210D1B83ACD79B006BCF7DB247ED002A4
5FC892C42720390BFA6AE21AEA8DC
TOTAL_AUTHBIN=2
```

Display CTE Build Information

To see the CTE build version, use the `vmsec version` command. For example:

```
 vmsec version
version 7
2020-07-31 10:03:59 (PDT)
Copyright (c) 2009-2022, Thales. All rights reserved.
```

Display Contents of Conf files

To display the contents of the `agent.conf` and `.agent.conf.defaults` files, use the `vmsec vmdconfig` command. For example:

```
 vmsec vmdconfig
appender_syslogdest_Syslog_Appender_0=127.0.0.1
VMSDK_AGENT_CONFIG_FILE=/opt/vormetric/DataSecurityExpert/agent/vmd/
etc/agent.conf
appender_layout_Syslog_Appender_0=Syslog_Layout
VMSDK_AGENT_VERSION=7.2.0.128
VMSDK_AGENT_BUILD_ID=28
PREV_URLS=https://srv.my.thales.com:8443
syslog_appender_myhost name=dev.my.thales.com
```

```
VMD_PORT=7024
...
...
appenders=Upload_Appender, File_Appender, Syslog_Appender_0
layouts=Upload_Layout, File_Layout, Syslog_Layout, Simple
CONNECT_TIMEOUT=180000
URL=https://srv.my.thales.com:8443
STRONG_ENTROPY=false
```

Configuring Dynamic Host Settings for AIX

Previously, when host settings were changed, currently executing processes for the specified images were not modified. Only when a new process started would the changed host settings take effect. To make an already running process use the new host setting values, you had to terminate the process and restart it. The Dynamic Host Setting feature now permits the modified host settings take effect when the new entries are pushed from the CipherTrust Manager to the agent.

If the Dynamic Host Setting feature is enabled, then when a host setting is altered, all running processes with that signature are affected and their existing security attributes are modified to the new host settings parameters. Future actions by a process will contain authorization(s) derived from the new attributes. It is important to note that all descendent processes are affected by a process's host setting change. If an existing host setting entry is modified, the same situation occurs.

If an existing process did not have a host setting and one is applied, then all processes with that signature are updated with the new values. All of the existing descendent processes are affected by the changes. New child processes inherit the host setting parameters and authorizations.

In v7.2 of CTE, three new `vmadmin` commands are provided to enable, disable, and report the status of the Dynamic Host Settings:

- To turn on dynamic host settings, type:

```
voradmin secfs config dhs_on 1
```

Note

You must restart the agent for this to setting to take effect.

- To turn off dynamic host settings, type:

```
voradmin secfs config dhs_on 0
```

Note

You must restart the agent for this to setting to take effect.

- To report the state of the dynamic host settings, type:

```
voradmin secfs config dhs_state
```

Note

State information is added to the secfs.log file.

- To immediately enable dynamic host settings without restarting the agent, type:

```
voradmin cmd dhs_enable
```

Note

You must restart the agent for this to setting to take effect. Perform this command after turning on DHS.

- To immediately disable dynamic host settings without restarting the agent, type::

```
voradmin cmd dhs_enable
```

Note

Restarting the agent will enable it unless you turn the dynamic host settings off first.

vmd utility

The `vmd` utility displays CTE software version information.

The `vmd` utility is located in `/opt/vormetric/DataSecurityExpert/agent/vmd/bin` and a symbolic link to this file is placed in `/usr/bin/vmd`.

Syntax

`vmd [OPTIONS...]`

`-h` show utility syntax

`-v` display CTE version

`-f` runs `vmd` in the foreground

Display the Installed Version

To display the installed CTE version, type:

```
 vmd -v
Version 7
<Release.build-number>
2022-02-04
Copyright (c) 2009-2022, Thales.. All rights reserved.
```

Upgrading CTE on AIX

This chapter describes how to upgrade an existing VTE for AIX host to CipherTrust Transparent Encryption (CTE) for AIX.

Scheduling a CTE Agent Upgrade

You can schedule an upgrade of the CTE Agent to occur the next time the server on which a CTE Agent is installed reboots normally. Scheduling an upgrade can minimize CTE service interruptions and reduce coordination issues in organizations where the security roles are separated.

Note

Scheduled upgrade on reboot is available in VTE for AIX version 5.3.0 GA and onwards. You cannot schedule an upgrade from an earlier version of VTE to version 5.3.0 GA or to CTE version .

Before You Begin

Keep in mind the following prerequisites for using scheduled upgrade, usage notes, and how scheduled upgrade behaves when errors occur:

- If a crash/power failure occurs before a user-initiated reboot, the scheduled upgrade runs when the system comes up after the crash/power failure.
- CipherTrust Manager connectivity is required during the scheduled upgrade process.
- All databases must be configured to automatically stop before CTE services stop during reboot/shutdown.
- Stopping and restarting the CTE Agent does not trigger a scheduled upgrade.
- The installation binary used to run the scheduled upgrade is stored in `/var/tmp` until the scheduled upgrade runs. Ensure that no scheduled maintenance jobs periodically delete files in `/var/tmp`. All temporary files used by scheduled upgrade are removed following a successful scheduled upgrade.

Using the Scheduled Upgrade Feature

Note

If a scheduled upgrade has been enabled but has not run because the system wasn't rebooted, you can override the existing scheduled upgrade with a newer CTE version by using the procedure described here with the newer installation binary.

1. Verify that the version of CTE you currently have installed is eligible for scheduled upgrade:

```
vmd -v
```

The version listed must be version 5.3.0 or later.

2. Log in as root, change to the directory containing the installation binary, and run the binary with the `-u` scheduled upgrade option. For example:

```
./vee-fs-7.2.0-56-aix71.bin -u
```

The following upgrade confirmation is displayed:

```
upgrade on reboot configured
```

> **Note**
>
> If syslog is properly configured, appropriate logs will be logged in syslog.

3. When you are ready, reboot the server.

```
shutdown -Fr
```

When the system restarts, the scheduled upgrade runs without any intervention needed.

4. After the system is up and running, log in and run `vmd -v` to verify that the new version has been installed.

Performing an Upgrade Manually When an Upgrade is Already Scheduled

If you want to upgrade without waiting for the system to reboot, follow these steps to perform an upgrade manually when a scheduled upgrade is already enabled:

1. Log in as root, change to the directory containing the installation binary, and run the binary without the `-u` scheduled upgrade option. For example:

```
./vee-fs-7.2.0-56-aix71.bin
```

The following upgrade confirmation is displayed:

```
upgrade on reboot pending
do you wish to continue [y/n]: y
```

2. Enter “Y” to cancel the scheduled upgrade and proceed with an immediate installation. If you enter “N”, the scheduled upgrade remains enabled and occurs on the next reboot.
   If you enter “Y”, the binary runs and displays the license agreement.
3. When prompted, enter “Y” to accept the license agreement or “N” to exit.
   After accepting the license agreement, the normal upgrade proceeds, the scheduled upgrade is canceled, and temporary files used by the scheduled upgrade are removed.

Uninstalling CTE from AIX

Considerations

- The CTE Agent must be removed from the AIX 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:
   - 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.

- Make sure the Agent and System locks have been disabled for the host.
- Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

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

5. Start the uninstall. Type:

```
/opt/vormetric/DataSecurityExpert/agent/vmd/bin/uninstall
Would you like to uninstall the vee-fs package? (Y/N) [Y]: Y
.............
Success!
```

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.