THALES

CipherTrust Transparent Encryption

CTE Agent for AIX Installation and Configuration Guide

Release 7.0.0

Document Version 1

September 22, 2020

CTE Agent for AIX Installation and Configuration Guide
7.0.0
Document Version 1
September 22, 2020

Contents

Preface

The CTE Agent for AIX Installation and Configuration Guide provides information about advanced installation, configuration, and integration options for CTE for AIX.

The CTE Agent Documentation Set

The following guides are available for CTE Agent:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.0.0.47*
- *Release Notes for CTE for Windows Version 7.0.0.47*
- *Release Notes for CTE for AIX Version 7.0.0.11*

Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

Table 3-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options.	Click the **System** tab and select **General** Preferences.
bold italic monospaced font	variables or text to be replaced	https://<***Token Server name***>/admin/ Enter password: <***Password***>
`regular monospacedfont`	Command and code examples XML examples	Example: `session start iptarget=192.168.253.102`

Table 3-1: Typographical Conventions (continued)

Convention	Usage	Example
italic regular font	GUI dialog box titles	The *General Preferences* window opens.
	File names, paths, and directories	*/usr/bin/*
	Emphasis	*Do not* resize the page.
	New terminology	*Key Management Interoperability Protocol (KMIP)*
	Document titles	See *CTE Agent for AIX Installation and Configuration Guide* for information about CipherTrust Transparent Encryption.
quotes	File extensions Attribute valuesTerms used in special senses	".js", ".ext" "true" "false", "0" "1+1" hot standby failover

Notes, tips, cautions, and warnings

Notes, tips, cautions, and warning statements may be used in this document.

A Note provides guidance or a recommendation, emphasizes important information, or provides a reference to related information. For example:

> **Note**
> It is recommended to keep tokenization keys separate from the other encryption/decryption keys.

A tip is used to highlight information that helps you complete a task more efficiently, such as a best practice or an alternate method of performing the task.

> **Tip**
> You can also use Ctrl+C to copy and Ctrl+P to paste.

Caution statements are used to alert you to important information that may help prevent unexpected results or data loss. For example:

CAUTION
Make a note of this passphrase. If you lose it, the card will be unusable.

A warning statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data. For example:

WARNING
Do not delete keys without first backing them up. All data that has been encrypted with deleted keys cannot be restored or accessed once the keys are gone.

Sales and Support

If you encounter a problem while installing, registering, or operating this 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.

For support and troubleshooting issues:

- https://supportportal.thalesgroup.com
- (800) 545-6608

For Thales Sales:

- https://cpl.thalesgroup.com/
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Chapter 1: 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. **Note** 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/.
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. Thales offers two key managers for use with CTE, the Vormetric Data Security Manager (DSM) and CipherTrust Manager.
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. The difference comes from the key manager you are using. The DSM refers to the machines as hosts, while the CipherTrust Manager refers to them as clients.
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.

  Thales offers two key managers that work with CTE:

  - CipherTrust Manager, Thales's next generation key manager.
  - The *Vormetric Data Security Manager* (DSM), Thales's legacy key manager.

Both key managers support all CTE for AIX features and can be set up as either a security-hardened physical appliance or a virtual appliance. Both provide access to the protected hosts though a browser-based, graphical user interface as well as an API and a CLI. Thales recommends that you use the CipherTrust Manager.

You must select one and only one key manager per host or host group. While you could have some hosts registered with a CipherTrust Manager and some registered with a DSM, you cannot have the same host registered to both a CipherTrust Manager and a DSM.

> **Note:** For a list of CTE versions and supported operating systems, see the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

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 DSM or CipherTrust 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.

Chapter 2: Getting Started with CTE for AIX

This chapter 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 sections:

Installation Workflow

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

1. Select which key manager you want to use. The Vormetric Data Security Manager and the CipherTrust Manager have different requirements, so you must make this decision first. For details, see "CTE Components" on page 11.
2. If you want to include the CTE Agent software with the AIX distribution files, see "AIX Package Installation" on the next page.
3. If you want to install the CTE Agent without registering with a key manager, see "Installing CTE with No Key Manager Registration" on the next page. However, you cannot protect any data on the host until it has been registered.

   Otherwise, set up your systems according to the requirements of the selected key manager. For details, see one of the following:

   - "Configuring CTE for AIX with CipherTrust Manager" on page 15
   - "Configuring CTE for AIX with a DSM" on page 26
4. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see one of the following:
   - "Guarding a Device with CipherTrust Manager" on page 21.
   - "Guarding a Device with the DSM" on page 45.

Additional Consideration: Tracking and Preventing Local User Creation

CTE allows you to track attempts to change user authentication files using the host settings `audit` and `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 audits access to the system credential files but does not prevent account creation.
- The `protect` setting both audits and prevents local user account creation. You must manually enable the `protect` setting for tracking and prevention of local user account creation.

You can tag the following files with either `audit` or `protect`. If you tag a file with both options, CTE uses the `protect` setting.

- `/etc/passwd`
- `/etc/group`

Notes

- 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.
- To see the audit messages in the DSM, you must use DSM version 6.x or later. Audit messages are not available in DSM versions 5.x and earlier.

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-7.0.0-11-aix71.bin -e
   Contents extracted.
   # ls *bff
   vee-fs-7.0.0-11-aix71.bff
   ```

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

   ```
   # installp -aX -d vee-fs-7.0.0-11-aix71.bff vee.fs
   ```

   For details about the installation and registration process, see the appropriate installation procedure.

   - If you are going to register the system with a CipherTrust Manager, see "Configuring CTE for AIX with CipherTrust Manager" on the facing page.
   - If you are going to register the system with a Vormetric Data Security Manager (DSM), see "Configuring CTE for AIX with a DSM" on page 26.

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" on page 11.

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-7.0.0-11-aix71.bin
   ```

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

   ```
   # ./vee-fs-7.0.0-11-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-7.0.0-11-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: 7.0.0.11

In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
    1) you must know the host name of the machine running the
       DSM (the host name is displayed on the
       Dashboard window of the Management Console), and
    2) unless you intend to use the 'shared secret' registration method,
       the agent's host machine must be pre-configured on the DSM as a
       host with the 'Reg. Allowed' checkbox enabled for this agent type
       on the Hosts window of the Management Console.

In order to register with a 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 one of the following:

   - "Configuring CTE for AIX with CipherTrust Manager" below
   - "Configuring CTE for AIX with a DSM" on page 26

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. If you want to register CTE with a Vormetric Data Security Manager (DSM), see "Configuring CTE for AIX with a DSM" on page 26.

Installation Overview

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

1. Gather the information needed for the install and set up your network as described in "Installation Prerequisites" on the next page.
2. Install CTE on the protected host as described in "Interactive Installation on AIX" on page 17 or "Silent Installation on AIX" on page 19.
3. Register the protected host with CipherTrust Manager and make sure that they can communicate with each other. Registration can be done as part of the initial installation or at any point after the CTE Agent has been installed.

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" on the facing page.
- **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" on page 19.

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.

To verify if hardware association (cloning prevention) is enabled on an AIX host, on the command line enter the following:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/access
```

If you see `usehw:true`, then hardware association is enabled. If you see `usehw:false`, it's disabled.

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.
- Do not install CTE on network-mounted volumes such as NFS.
- 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-7.0.0-11-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 ifix from IBM. If the required ifix 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.
- If the system is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

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

The default port for communication between the 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.

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" on page 36).

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

Make sure you have the following information from the CM Administrator:

- The registration token for the CipherTrust Manager with which you plan to register the CTE Agent.
- The name of the profile you intend to assign to the client if you want to use a profile other than the default client profile.
- Optionally, the name of the host group 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-7.0.0-11-aix71.bin
   ```

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

   ```
   # ./vee-fs-7.0.0-11-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-7.0.0-11-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: 7.0.0.11

In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
    1) you must know the host name of the machine running the
       DSM (the host name is displayed on the
       Dashboard window of the Management Console), and
    2) unless you intend to use the 'shared secret' registration method,
       the agent's host machine must be pre-configured on the DSM as a
       host with the 'Reg. Allowed' checkbox enabled for this agent type
       on the Hosts window of the Management Console.

In order to register with a 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. 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

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 following
list.

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

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

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

```
Please enter the registration token: 12345
Please enter the profile name for this host: My-Profile
Please enter the host group name for this host, if any:
Please enter a description for this host: West Coast Datacenter server 5

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

8. At the hardware association prompt, select whether you want to enable the hardware association feature (for details, see "Hardware Association (Cloning Prevention) Option" on page 16). 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
```

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 File System Agent with the
CipherTrust Manager on 10.3.200.141.

Installation success.
```

10. 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.

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

Make sure you have the following information from the CM Administrator:

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

Parameter	Description
SERVER_HOSTNAME	Required if you want to register CTE with a CipherTrust Manager.
REG_TOKEN	The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.

Parameter	Description
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.
HOST_DOMAIN	Specifies the domain name with which this CTE Agent will be associated.
HOST_GROUP	Specifies the optional client group with which this client will be associated.
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.
PKCS11_PASSWORD	The administrative password for the CTE Agent. Required if the CTE Agent is being registered with a CipherTrust Manager. This password allows users to access encrypted data on the client if it is disconnected from the CipherTrust Manager.
AGENT_USEIP	Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.
HOST_DESC	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.
AGENT_HOST_PORT	Specifies the port number this CTE Agent should use.
USEHWSIG	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.

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

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
REG_TOKEN=12345
PKCS11_PASSWORD=ClientAdminP@$$w0rd
```

3. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.
4. 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-7.0.0-11-aix71.bin -s /tmp/unattended.txt
   ```

5. 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`.
6. 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.

Guarding a Device with CipherTrust Manager

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

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

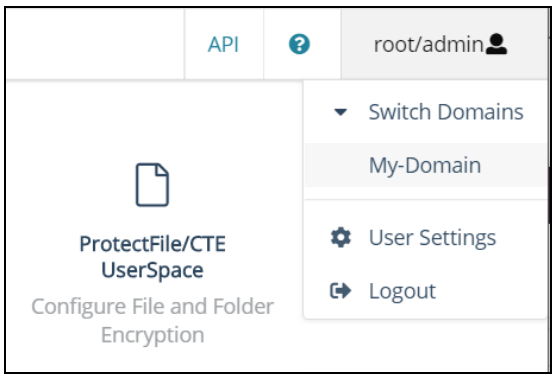
1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to 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" on the next page. If you need to change to a different domain, do the following:
   a. In the top menu bar, click the user name **root/admin** on the right-hand side.
   b. Select **Switch Domains**, then select the domain in which the client is registered.
   c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

1. In the Applications page of the CipherTrust Manager Console, select **Keys & Access Management**.
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 Metadata > Groups for Key sharing** section, do the following:
   a. In the **Search** box, type "cte".
   b. Add CTE Admins and CTE Clients to the key sharing groups by clicking the green **Add** button. The **Key Shared?** check box is automatically selected and the **Add** button changes to a **Remove** button.
   c. Below the Groups table, click the **CTE Key Properties** check box.

   CipherTrust Manager displays the following options for CTE keys:

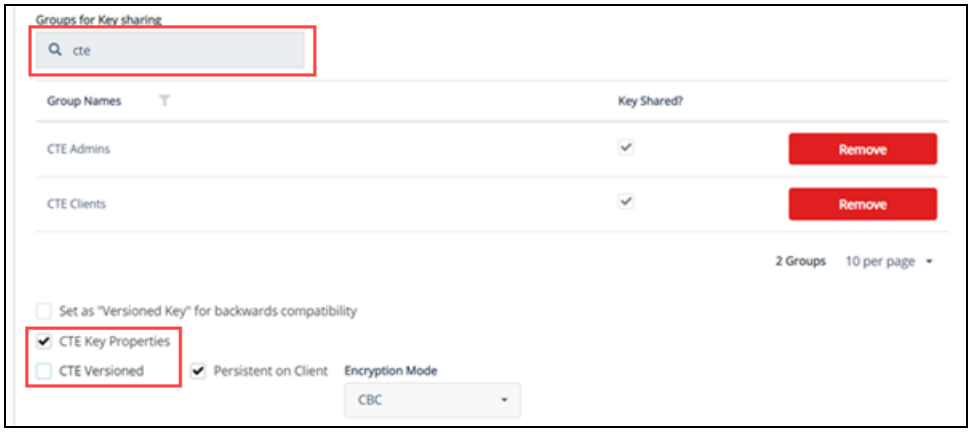
   - **CTE Versioned**: Specify whether the key is versioned. By default, the key is set as versioned.

     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.

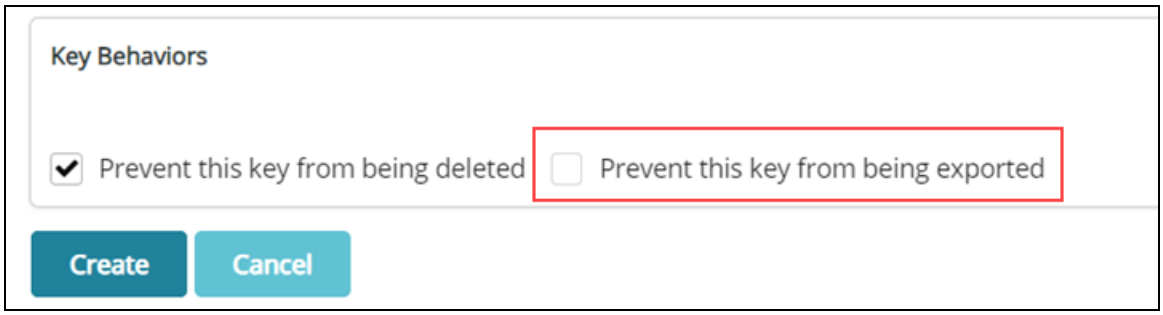
     When the check box is selected, the key is downloaded and stored (in an encrypted form) in persistent memory on the client.

     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*.



5. In the Key Behaviors section at the bottom of the page, clear the **Prevent this key from being exported** check box. If the key cannot be exported, the key will not appear in the keys list when you add the key rule to the policy.



6. Click **Create**. The new key appears in the Keys table.

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **CTE** 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/CTE-LDT 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 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. This rule is required by CTE-LDT, so you cannot edit it, move it, or delete it.

   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.

   For this example, click **Create Security Rule** and:

   - Set Action to all_ops.
   - Set Effect to **Permit** and **Audit**.

   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**.

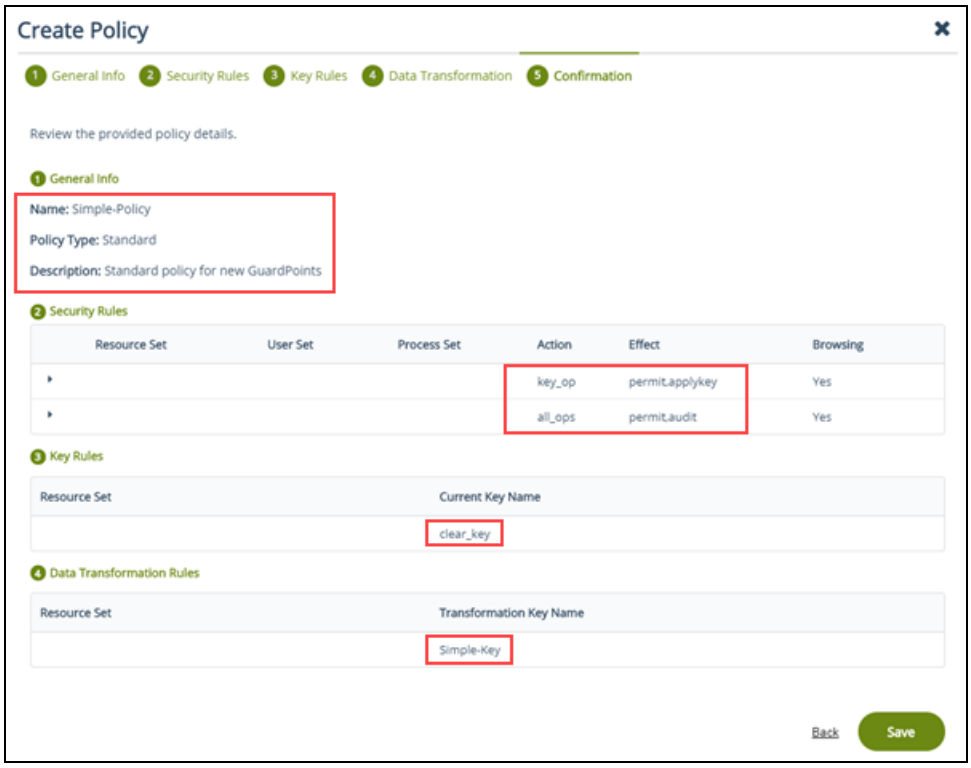
7. On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

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 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" on page 22.

   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:

   > **Tip:** If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

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 CipherTrust Manager pushes the GuardPoint configuration to the client and CTE immediately beings transforming the data in the specified folders from clear-text to cipher-text.
6. When the data transformation has finished, applications can resume accessing the now-protected data.

Configuring CTE for AIX with a DSM

This section describes how to install and configure CTE on AIX systems that you plan to register with a Vormetric Data Security Manager (DSM). This process requires actions from two roles:

- The *agent installer* or *host administrator* who uses these instructions to install and configure the CTE Agent on each AIX host whose data you want to protect.
- The DSM Administrator, who adds hosts to the DSM database using the FQDN or the IP address.

Installation Overview

The installation and configuration process for CTE with a DSM consists of three basic steps:

1. Gather the information needed for the install and set up your network as described in "Installation Prerequisites" below.
2. Select the installation options you want to use as described in "Installation and Registration Options" on page 28.
3. Install CTE on the protected host as described in "Interactive Installation on AIX" on page 29 or "Silent Installation on AIX" on page 36.
4. Register the protected host with the DSM and make sure that they can communicate with each other. This process can be done as part of the initial installation or at any point after the CTE Agent has been installed.

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.
- Do not install CTE on network-mounted volumes such as NFS.
- 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-7.0.0-11-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 ifix from IBM. If the required ifix 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 DSM(s) to all hosts where you install CTE.
- If the host is a virtual machine, the VM must be deployed and running.

Host Name Resolution Requirements

Host name resolution is the method of mapping a host name to an IP address. During this configuration process, enter either the FQDNs, or IP addresses, of your DSM and protected hosts. If you use FQDNs, your protected hosts must be able to resolve the DSM host names, and the DSM must be able to resolve its protected hosts.

> **Note**
> The exception to this requirement is if you plan to configure one-way communication between CTE and the DSM.

A Domain Name Service (DNS) server is the preferred method of host name resolution. If you use DNS, use the FQDNs for the DSM and hosts.

If you do *not* use a DNS, you can do one of the following:

- Use the IP addresses of the DSM and protected hosts.
- Add an entry in the `/etc/hosts` file on the DSM associated with the host. The administrator must use the CipherTrust CLI, and, in an HA environment, they must add an entry to *each* DSM in the cluster because entries in the `/etc/hosts` file are not replicated across the cluster.

Port Configuration Requirements

If a protected host must communicate with the DSM through a firewall, see the *DSM Administration Guide* to determine which of the ports must be opened through the firewall.

The default port for communication between the DSM and the CTE Agent is 7024. If this port is already in use, you can set the port to a different number during the CTE Agent installation.

One-way Communication Option

In some deployments, CTE might not be visible to the DSM through normal network communications. For example, when the host on which CTE is installed:

- is behind NAT.
- is behind a firewall.
- is not permanently connected to a communication channel to the DSM.
- is unable to resolve the host name to an IP address.

In these situations, CTE can initiate CTE-only communication to the DSM. This feature is called one-way communication and works by having CTE poll the DSM for any policy messages or changes, then downloading changes as required.

The downside of one-way communication is that the DSM cannot issue any queries to CTE. For example, the DSM Administrator cannot browse host directories or User IDs. To enable the full functionality of both CTE and the CipherTrust Manager, Thales recommends that you use two-way communication between them whenever possible.

Port Usage in One-Way Communications Mode

By default, polling from the agent host to the DSM when running in one-way communications mode uses HTTP via port 8080. If the CTE Agent is configured to use secure polling, then polling is performed using HTTPS via port 8448 (in suite B mode) or port 8445.

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, so you should decide what options you want to use before you start the installation.

Installation Method Options

There are two methods for installing CTE on AIX platforms:

- **Interactive:** 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" on the facing page.
- **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" on page 36.

CTE Registration Method Options

You can register the protected hosts with a DSM using either the *Fingerprint method* or the *Shared Secret method*.

- **Fingerprint method** requires the DSM Administrator to add the FQDN, or IP address, of each protected host to the DSM before registering CTE.

  During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. The security administrator must verify the fingerprint to make sure the certificate is valid.

- **Shared Secret method** requires the DSM Administrator to create a *shared secret* password—a case-sensitive string of characters—for auto-registering a domain or host group.

  CTE installers use the shared secret to add and register protected hosts to the DSM for a domain or host group. The DSM Administrator can optionally add host names or IP addresses to the DSM. There is no need to verify that the protected host and DSM share valid certificates. You can add multiple protected hosts dynamically with a single shared secret password during CTE installation and registration.

  After the DSM Administrator creates a shared secret for the domain or host group in which the new protected host will reside, obtain it and the validity period (one hour, day, week, or month) and register within that period.

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 hosts.

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

To verify if hardware association (cloning prevention) is enabled on an AIX host, on the command line enter the following:

```
cat /opt/vormetric/DataSecurityExpert/agent/vmd/etc/access
```

If you see `usehw:true`, then hardware association is enabled. If you see `usehw:false`, it's disabled.

CTE AIX Installation Checklist

Use the following table to verify prerequisites and collect the information you need for the installation.

Checklist item	Notes

Obtain the CTE Agent installation image from Thales. The format for the installation file names is:
`vee-fs-<release>-<build>-<system>.bin`
For example:
`vee-fs-7.0.0-11-aix71.bin`	

Get the Fully Qualified Domain Name (FQDN) of the DSM as shown on the DSM Dashboard.	
Get the IP address or FQDN of the host. If you are using the Fingerprint registration method, this must match exactly with the name specified in the DSM.	
Make sure you have the `root` user login credentials for the host. You must install CTE as `root`.	
If using Shared Secret registration, obtain the following from the DSM Administrator: • Shared secret password • Domain • Host group, if applicable • Description of the host (Optional)	
If using the Fingerprint registration method: • Ask the DSM Administrator to add the host to the DSM and check the **Registration Allowed** and **Communication Enabled** check boxes. • Get the EC CA certificate fingerprint as shown on the DSM Dashboard.	
Make sure the host can communicate with the DSM. For details, see "Host Name Resolution Requirements" on page 27.	
Make sure the correct ports are open. For details, see "Port Configuration Requirements" on page 27.	
Determine if you want to use the One-way communication option. For details, see "One-way Communication Option" on page 27.	
Determine if you want to use the Hardware Association feature. For details, see "Hardware Association (Cloning Prevention) Option" on the previous page.	
Synchronize the host clock to the DSM clock.	
Determine your preferred DNS Server (if using FQDNs).	

Interactive Installation on AIX

The AIX interactive install is a standard 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" on page 36).

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

The procedure for installing CTE depends on the registration method you want to use. The available methods are described in "CTE Registration Method Options" on page 28. After you have selected your registration method, you can use one of the following procedures:

- "Installing CTE and Registering Using the Shared Secret Registration Method" on page 33
- "Installing CTE and Registering Using the Certificate Fingerprint" below

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

Installing CTE and Registering Using the Certificate Fingerprint

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a DSM using the Fingerprint registration method. For more information about the available registration methods, see "CTE Registration Method Options" on page 28.

For other installation options, see "Installing CTE and Registering Using the Shared Secret Registration Method" on page 33 and "Installing CTE with No Key Manager Registration" on page 14.

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

> **Note**
> If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

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-7.0.0-11-aix71.bin
   ```

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

   ```
   # ./vee-fs-7.0.0-11-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-7.0.0-11-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.

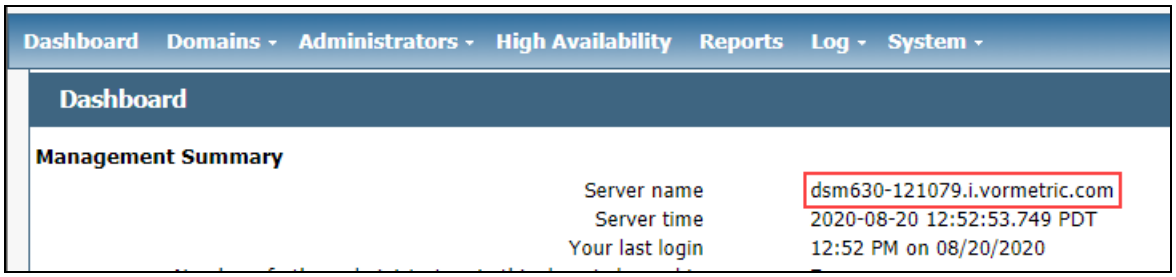
   Agent Type: CipherTrust Transparent Encryption File System Agent
   Agent Version: 7.0.0.11

   In order to register the CipherTrust Transparent Encryption File System Agent
   with a Vormetric Data Security Manager
       1) you must know the host name of the machine running the
          DSM (the host name is displayed on the
          Dashboard window of the Management Console), and
       2) unless you intend to use the 'shared secret' registration method,
          the agent's host machine must be pre-configured on the DSM as a
          host with the 'Reg. Allowed' checkbox enabled for this agent type
          on the Hosts window of the Management Console.

   In order to register with a 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 name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

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

Please enter the primary key manager host name: dsm630-121079.i.vormetric.com

You entered the host name dsm630-121079.i.vormetric.com
Is this host name correct? (Y/N) [Y]: Y
```

6. Enter the host name when prompted. This name must match the name used on the **Add Host** page of the DSM Management Console.

```
Please enter the host name of this machine, or select from the following list. If using the
"fingerprint" registration method, the name you provide must precisely match the name used
on the "Add Host" page of the Management Console.

[1] host14.i.example.com
[2] Host-AIX71.i.example.com
[3] 10.3.14.90

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 3
You selected "10.3.14.90".
```

7. When prompted for the registration method, enter **F** for fingerprint registration:

```
Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: F
```

8. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. 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
```

9. At this point, the install program generates certificate signing requests and lists the fingerprint of the EC (elliptic curve) CA (Certificate Authority) certificate. This fingerprint must match the one on the DSM Dashboard in the **Management Summary** section, **EC CA fingerprint** field.

```
The following is the fingerprint of the EC CA certificate.
Please verify that it matches the fingerprint shown on the Dashboard
page of the Management Console.  If they do not match, it can indicate an
unsuccessful setup or an attack.

2F:9A:1C:DB:7E:B9:6C:63:D4:BA:D2:25:C6:7C:97:F1:E1:48:20:AE

Do the fingerprints match? (Y/N) [N]: Y
```

   If the fingerprints match, enter `Y`. The installer displays the fingerprint for the CTE Agent on the host and completes the installation:

```
The following is the fingerprint for this agent on this host.
Please verify that it matches the fingerprint shown for this host on the
Edit Host window of the Management Console.

12:CF:64:A3:28:7E:2E:50:72:70:FF:8F:B2:79:5B:4F:40:1B:74:20

Successfully registered the CipherTrust Transparent Encryption File System Agent with the
Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.

Installation success.
```

10. Verify with the DSM Administrator that the CTE fingerprint matches with the fingerprint shown for this host on the **Hosts > Hostname > Edit Host** window of the DSM Management Console. CTE is installed and registered.
11. Verify the installation by checking the CTE processes on the host:
    - Run `vmd -v` to check the version of CTE.
    - Run `vmsec status` to display the CTE processes.
    - Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Installing CTE and Registering Using the Shared Secret Registration Method

The following procedure describes how to install the CTE Agent on the AIX host and then register the CTE Agent with a DSM using the Shared Secret registration method. For more information about the available registration methods, see "CTE Registration Method Options" on page 28.

For other installation options, see "Installing CTE and Registering Using the Certificate Fingerprint" on page 30 and "Installing CTE with No Key Manager Registration" on page 14.

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

> **Note**
> If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

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-7.0.0-11-aix71.bin
   ```

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

   ```
   # ./vee-fs-7.0.0-11-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-7.0.0-11-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.

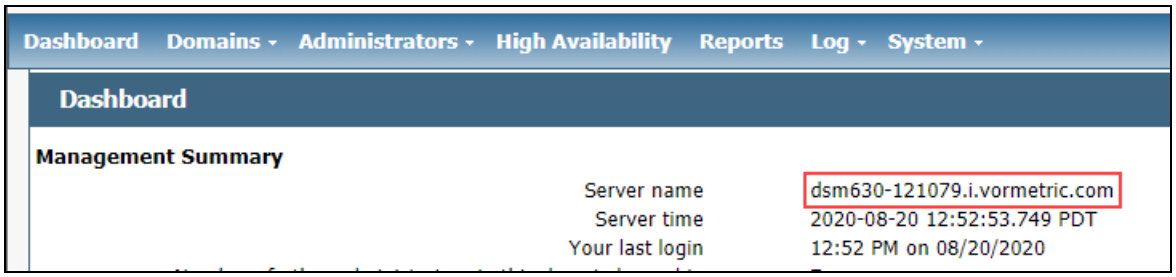
   Agent Type: CipherTrust Transparent Encryption File System Agent
   Agent Version: 7.0.0.11

   In order to register the CipherTrust Transparent Encryption File System Agent
   with a Vormetric Data Security Manager
       1) you must know the host name of the machine running the
          DSM (the host name is displayed on the
          Dashboard window of the Management Console), and
       2) unless you intend to use the 'shared secret' registration method,
          the agent's host machine must be pre-configured on the DSM as a
          host with the 'Reg. Allowed' checkbox enabled for this agent type
          on the Hosts window of the Management Console.

   In order to register with a 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 name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

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

Please enter the primary key manager host name: dsm630-121079.i.vormetric.com

You entered the host name dsm630-121079.i.vormetric.com
Is this host name correct? (Y/N) [Y]: Y
```

6. Enter the host name when prompted. If the Shared Secret registration in your DSM is configured to require an existing host entry, his name must match the name used on the **Add Host** page of the DSM Management Console.

```
Please enter the host name of this machine, or select from the following list. If using the
"fingerprint" registration method, the name you provide must precisely match the name used
on the "Add Host" page of the Management Console.

[1] host14.i.example.com
[2] Host-AIX71.i.example.com
[3] 10.3.14.90

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 3
You selected "10.3.14.90".
```

7. When prompted for the registration method, enter s for shared secret registration and then enter the required information about the domain, optional host group, and optional host description. For example:

```
Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: S

What is the registration shared secret?
Please enter the domain name for this host: west-coast-domain
Please enter the host group name for this host, if any:
Please enter a description for this host: West Coast Data Center server 5

Shared secret    : ************
Domain name      : west-coast-domain
Host Group       : (none)
Host description : West Coast Data Center 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 that prevents a clone of this machine from accessing keys in the DSM. 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
```

9. At this point the installation script completes the installation and indicates that it successfully registered the host with the DSM.

```
Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent with the
Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.
```

10. Verify the installation by checking the CTE processes on the host:
    - Run `vmd -v` to check the version of CTE.
    - Run `vmsec status` to display the CTE processes.
    - Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

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 DSM you specify in the silent installation file.

For details, see one of the following procedures:

- "Silent Installation on AIX Using the Shared Secret Registration Method" below
- "Silent Installation on AIX Using the Fingerprint Registration Method" on page 38

Silent Installation on AIX Using the Shared Secret Registration Method

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 DSM you specify in the silent installation file using the Shared Secret registration method. To register it using the Fingerprint registration method, see "Silent Installation on AIX Using the Fingerprint Registration Method" on page 38.

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

> **Note**
> If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

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:

Parameter	Description
`SERVER_HOSTNAME`	Required if you want to register CTE with a DSM.
`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.
`SHARED_SECRET`	Specifies the shared secret for the DSM. This value is required for shared secret registration.
`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.
`PKCS11_PASSWORD`	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
`AGENT_USEIP`	Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.
`HOST_DESC`	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.
`AGENT_HOST_PORT`	Specifies the port number this CTE Agent should use.
`USEHWSIG`	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.

Parameter	Description
ONEWAY_COMMS	Set this value to 1 when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

The following example contains just the required information for Shared Secretregistration. In this case, the host will be registered wtih the DSM using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
SHARED_SECRET=Shallacl12345#
HOST_DOMAIN=My-Domain
```

3. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.
4. 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-7.0.0-11-aix71.bin -s /tmp/unattended.txt
   ```

5. 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`.

Silent Installation on AIX Using the Fingerprint Registration Method

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 DSM you specify in the silent installation file using the Fingerprint registration method. To register using the Shared Secret registration method, see "Silent Installation on AIX Using the Shared Secret Registration Method" on page 36.

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

Note
If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

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:

Parameter	Description
SERVER_HOSTNAME	Required if you want to register CTE with a DSM.
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.
PKCS11_PASSWORD	The administrative password for the CTE Agent. This password allows users to access encrypted data on the host if it is disconnected from the DSM.
AGENT_USEIP	Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.
HOST_DESC	Specifies a description for the host. This description is displayed in the DSM. If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.
AGENT_HOST_PORT	Specifies the port number this CTE Agent should use.
USEHWSIG	Set this value to 1 when you want to associate this installation with the machine hardware for cloning prevention.
ONEWAY_COMMS	Set this value to 1 when CTE-initiated-only communication is required. Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

The following example contains just the required information for Fingerprint registration. In this case, the host will be registered wtih the DSM using its IP address instead of its host name:

```
SERVER_HOSTNAME=Key-Mgmt-Server.example.com
```

3. Copy or mount the CTE installation file to the host system. The installation file is in the format `vee-fs-<release>-<build>-<system>.bin`.

4. 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-7.0.0-11-aix71.bin -s /tmp/unattended.txt
   ```

5. 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`.

Registering CTE with the Shared Secret Registration Method After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see "Installing CTE and Registering Using the Shared Secret Registration Method" on page 33 or "Installing CTE and Registering Using the Certificate Fingerprint" on page 30.

Prerequisites

Make sure you know the following information from the DSM Administrator:

- The server name of the primary DSM as shown on the DSM Dashboard.
- The shared secret for the domain on the primary DSM with which you want to register the host.
- The name of the domain in the DSM with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.

All of this information is case-sensitive and must exactly match the corresponding information in the DSM.

> **Note**
> If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot register the CTE Agent without `root` access.
2. Launch the CTE Registration script by running the `register_host` script. The default location is `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`. For example:

   ```
   # ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host
   Welcome to the CipherTrust Transparent Encryption File System Agent
   Registration Program.

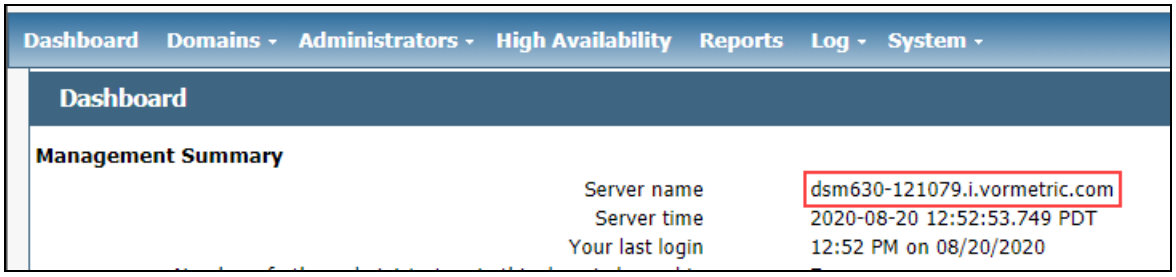
   Agent Type: CipherTrust Transparent Encryption File System Agent
   Agent Version: 7.0.0.11
   ```

```
In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
    1) you must know the host name of the machine running the
       DSM (the host name is displayed on the
       Dashboard window of the Management Console), and
    2) unless you intend to use the 'shared secret' registration method,
       the agent's host machine must be pre-configured on the DSM as a
       host with the 'Reg. Allowed' checkbox enabled for this agent type
       on the Hosts window of the Management Console.

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

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

3. Enter `Y` to continue with the registration process. The install script prompts you to enter the name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

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

Please enter the primary key manager host name: dsm630-121079.i.vormetric.com

You entered the host name dsm630-121079.i.vormetric.com
Is this host name correct? (Y/N) [Y]: Y
```

4. Enter the host name when prompted. If the Shared Secret registration in your DSM is configured to require an existing host entry, his name must match the name used on the **Add Host** page of the DSM Management Console.

```
Please enter the host name of this machine, or select from the following list. If using the
"fingerprint" registration method, the name you provide must precisely match the name used
on the "Add Host" page of the Management Console.

[1] host14.i.example.com
[2] Host-AIX71.i.example.com
[3] 10.3.14.90

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 3
You selected "10.3.14.90".
```

5. When prompted for the registration method, enter s for shared secret registration and then enter the required information about the domain, optional host group, and optional host description. For example:

```
Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: S

What is the registration shared secret?
Please enter the domain name for this host: west-coast-domain
Please enter the host group name for this host, if any:
Please enter a description for this host: West Coast Data Center server 5

Shared secret    : ************
Domain name      : west-coast-domain
Host Group       : (none)
Host description : West Coast Data Center server 5
Are the above values correct?  (Y/N) [Y]: Y
```

6. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. 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
```

7. At this point the installation script completes the installation and indicates that it successfully registered the host with the DSM.

```
Generating certificate signing request for the kernel component...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent with the
Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.
```

8. Verify the installation by checking the CTE processes on the host:
   - Run `vmd -v` to check the version of CTE.
   - Run `vmsec status` to display the CTE processes.
   - Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Registering CTE with the Fingerprint Registration Method After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see "Installing CTE and Registering Using the Certificate Fingerprint" on page 30 or "Installing CTE and Registering Using the Shared Secret Registration Method" on page 33.

Prerequisites

Make sure the DSM Administrator has added the the FQDN, or IP address, of this host to the domain in which you want to register the host. During the registration, the DSM generates the certificate and passes it down to CTE along with the fingerprint. You will then need to verify the certificate fingerprint as part of the registration procedure.

In the DSM Management Console, the entry for the host must have at least the **Registration Allowed Agents > FS** and **Communication Enabled** options selected.

When you register the host, the machine name you use must exactly match the one in the DSM.

Additionally, make sure you know the server name of the primary DSM as shown on the DSM Dashboard.

> **Note**
> If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host where you will install the CTE Agent as `root`. You cannot register the CTE Agent without `root` access.
2. Launch the CTE Registration script by running the `register_host` script. The default location is `/opt/vormetric/DataSecurityExpert/agent/vmd/bin`. For example:

```
# ./opt/vormetric/DataSecurityExpert/agent/vmd/bin/register_host
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.

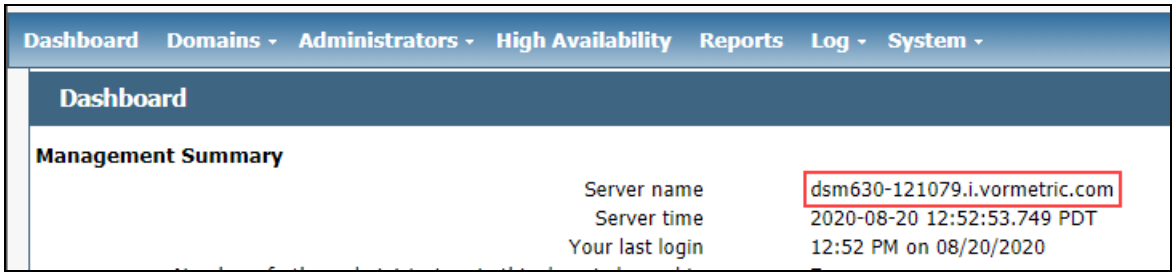
Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.0.0.11

In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
    1) you must know the host name of the machine running the
       DSM (the host name is displayed on the
       Dashboard window of the Management Console), and
    2) unless you intend to use the 'shared secret' registration method,
       the agent's host machine must be pre-configured on the DSM as a
       host with the 'Reg. Allowed' checkbox enabled for this agent type
       on the Hosts window of the Management Console.

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

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

3. Enter **`Y`** to continue with the registration process. The install script prompts you to enter the name of the DSM with which you want to register the host. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



For example:

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

Please enter the primary key manager host name: dsm630-121079.i.vormetric.com

You entered the host name dsm630-121079.i.vormetric.com
Is this host name correct? (Y/N) [Y]: Y
```

4. Enter the host name when prompted. This name must match the name used on the **Add Host** page of the DSM Management Console.

```
Please enter the host name of this machine, or select from the following list. If using the
"fingerprint" registration method, the name you provide must precisely match the name used
on the "Add Host" page of the Management Console.

[1] host14.i.example.com
[2] Host-AIX71.i.example.com
[3] 10.3.14.90

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 3
You selected "10.3.14.90".
```

5. When prompted for the registration method, enter **F** for fingerprint registration:

```
Would you like to register to the DSM using a
registration shared secret (S) or using fingerprints (F)? (S/F) [S]: F
```

6. At the hardware association prompt, select whether you want to enable the hardware association feature that prevents a clone of this machine from accessing keys in the DSM. 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
```

7. At this point, the install program generates certificate signing requests and lists the fingerprint of the EC (elliptic curve) CA (Certificate Authority) certificate. This fingerprint must match the one on the DSM Dashboard in the **Management Summary** section, **EC CA fingerprint** field.

```
The following is the fingerprint of the EC CA certificate.
Please verify that it matches the fingerprint shown on the Dashboard
page of the Management Console.  If they do not match, it can indicate an
unsuccessful setup or an attack.

2F:9A:1C:DB:7E:B9:6C:63:D4:BA:D2:25:C6:7C:97:F1:E1:48:20:AE

Do the fingerprints match? (Y/N) [N]: Y
```

   If the fingerprints match, enter **Y**. The installer displays the fingerprint for the CTE Agent on the host and completes the installation:

```
The following is the fingerprint for this agent on this host.
Please verify that it matches the fingerprint shown for this host on the
Edit Host window of the Management Console.

12:CF:64:A3:28:7E:2E:50:72:70:FF:8F:B2:79:5B:4F:40:1B:74:20

Successfully registered the CipherTrust Transparent Encryption File System Agent with the
Vormetric Data Security Manager on dsm630-121079.i.vormetric.com.

Installation success.
```

8. Verify with the DSM Administrator that the CTE fingerprint matches with the fingerprint shown for this host on the **Hosts > Hostname > Edit Host** window of the DSM Management Console. CTE is installed and registered.

9. Verify the installation by checking the CTE processes on the host:
   - Run `vmd -v` to check the version of CTE.
   - Run `vmsec status` to display the CTE processes.
   - Look at the log files in `/var/log/vormetric/install.fs.log.<date>`, especially `vorvmd_root.log`.

Guarding a Device with the DSM

After you register a device with a DSM, you can create as many GuardPoints on the device as you need. These GuardPoints can protect the entire device or individual directories or files.

In order to guard a device, you need to use the DSM Management Console to:

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

The following example creates a simple policy with a single key rule and no access controls and uses it to guard several directories on a registered host. For all of the following procedures, you must be logged into the DSM Management Console as a DSM Administrator, and you must be in the domain with which the host is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the *DSM Administration Guide*.

Access the DSM Domain

1. In a web browser, navigate to the URL of the DSM you want to use and log in with DSM Administrator credentials.
2. In the top menu bar of the DSM Management Console, select **Domains > Switch Domains**.
3. Select the domain with which the host you want to protect is registered and click **Switch to domain**.

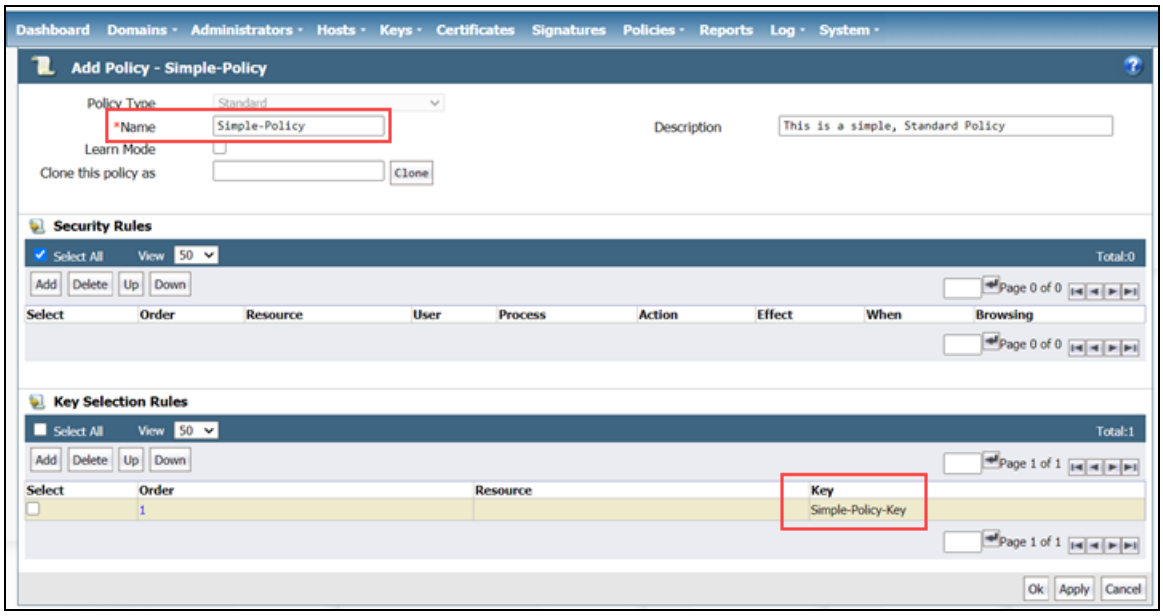
Create an Encryption Key

1. In the top menu bar of the DSM Management Console, select **Keys**.
2. In the Key table, click **Add**
3. In the **Name** field, add a name for the key. This name must be unique. For example, Simple-Policy-Key.
4. Set any other desired options or use the defaults provided.
5. Click **Ok**.

Create a Standard Policy

1. In the top menu bar, select **Policies**.
2. In the Policy table, click **Add**.
3. In the Add Policy page:

a. Select a Policy Type. In this example, we will create a Standard policy.
b. Enter a name for the policy in the **Name** field. For example, Simple-Policy.
c. Enter a description for the policy in the **Description** field.
d. In the Key Selection Rules section, click **Add**.
e. In the Key field, click **Select**.
f. Select the key you created earlier and click **Select key**.
g. Click **Ok**.



4. Click **Ok** to create the policy.

Create a GuardPoint

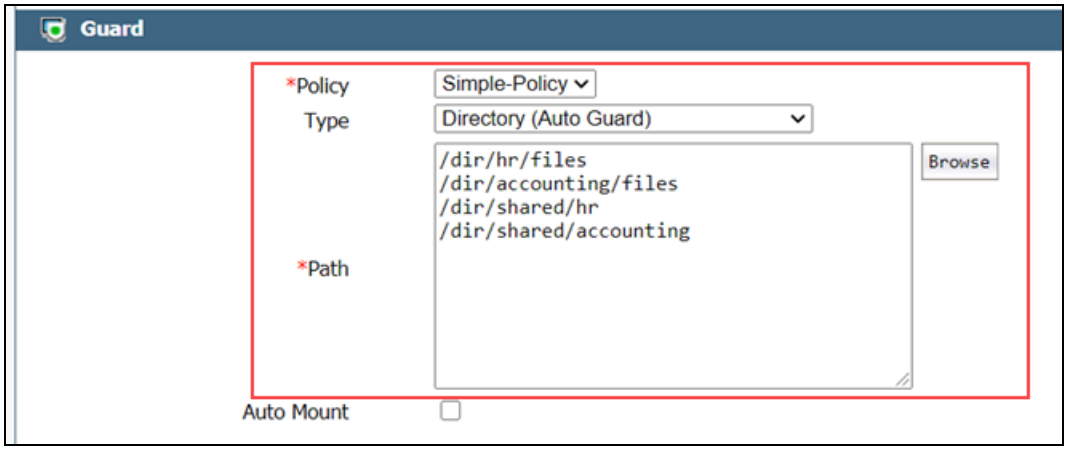
1. Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
   - /dir/hr/files
   - /dir/accounting/files
   - /dir/shared/hr
   - /dir/shared/accounting

   > **Tip:** If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

2. In the top menu bar, click **Hosts**.
3. In the Hosts table, click on the name of the host you want to protect.
4. Click the **GuardPoints** tab.
5. In the GuardPoints table, click **Guard**.

6. In the Guard 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 **Directory (Auto Guard)**.
   c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a Windows-style explorer.

      If you want to enter multiple paths, put each path on its own line. For example:



   d. Click **Ok**.

   The DSM pushes the GuardPoint configuration to the host and CTE immediately beings transforming the data in the specified folders from clear-text to cipher-text.

7. When the data transformation has finished, applications can resume accessing the now-protected data.

Chapter 3: Special Cases for CTE Policies

This chapter describes some CTE-specific configuration tasks related to configuring policies in the DSM and contains the following sections:

More Information About Configuring CTE Policies

This chapter describes some special cases that apply only to CTE agent policy configuration. See the DSM Administration Guide for general information about configuring polices. The following chapters in the *DSM Administration Guide* pertain specifically to the information in this chapter:

- “Creating and Configuring Signature Sets”
- “Configuring Hosts and Host Groups”
- “Configuring Policies”

Re-Signing Executable Files on Secfs GuardPoints

If any of your existing VTE for AIX hosts are running VTE versions prior to version 5.2.7, an issue affects signed executables in encryption policies. In these older VTE for AIX versions, any executable that is part of either a host setting, or Signature set, and resides in a GuardPoint that uses an encryption policy, will use different signatures in the case of a key rotation using Offline Data Transformation. So after each key rotation the host settings executables will no longer be authenticated, or the Signature Set policy rules that include those executables will no longer match them as expected. This problem occurred because VTE generated an SHA signature of the encrypted executable which changes after each key rotation. To work around these issues on these older VTE versions, the DSM Security Administrator must manually re-sign each affected executable after each key rotation. This workaround is *not* needed for any VTE for AIX release version 5.2.7 or later.

The SHA signature is created from the unencrypted executable. This new SHA signature does not change with a key rotation.

If upgrading or installing a new machine using the same signature sets that you used previously, do the following:

1. Install the current release of the CTE Agent. The previous signatures will be used until the next key rotation.
2. Before the next key rotation, the security administrator must resign the binaries.
3. Do not remove the old signatures on the DSM or CipherTrust Manager until all agents have been upgraded to the latest CTE release. Refer to the *DSM Installation and Configuration Guide* for information on how to perform a manual re-sign.
4. After all agents have been upgraded, then you can remove the old signatures.

> **Note**
> In previous releases, if the executable was in a GuardPoint protected directory, but was the same as an unguarded executable, the administrator could restrict only the guarded executable. In the current release of CTE, the unguarded executable matches the guarded executable with regards to policies.

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 to verify that the host settings is set to true:
   ```
   # vmsec vmdconfig
   ```

Restricting Access Overrides from Unauthorized Identities

In some setups, system administrators can use the host settings > |authenticator| feature with `su` to change identities and gain access to restricted data. Now, you can instruct CTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CTE 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.

CTE 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.

To restrict access overrides in the DSM:

1. At the DSM Management Console, click **Hosts > Hosts**.
2. Click on an existing host name to edit the host.
3. Click **Host Settings** tab.
4. Add the following to the host settings:

   `|path_no_trust|<path of the binary>`

   For example:

   `|path_no_trust|/bin/ksh`

   The above example indicates that no process under the kshell executable will be authenticated.
5. Click **OK.**

To restrict access overrides in CipherTrust Manager:

1. In the CipherTrust Manager Applications Page, click **CTE > Clients**.
2. Click on an existing client name to edit the client.
3. Click **Client Settings** tab.
4. Add the following to the client settings:

   `|path_no_trust|<path of the binary>`

   For example:

   `|path_no_trust|/bin/ksh`

   The above example indicates that no process under the kshell executable will be authenticated.
5. Click **OK.**

Chapter 4: Using CTE with Oracle

This chapter describes how to install and configure CTE on Oracle RAC ASM, as well as install and use CTE for AIX with Oracle Automated Storage Management (ASM™) Cluster File System (ACFS™) .

It contains the following sections:

CTE on ACFS Installation Overview

CTE enables data protection of ACFS on `secvm` volumes as part of the Oracle ASM stack. Oracle ACFS configured with `secvm` block devices is intended for use solely by the Oracle RAC application set to store related Oracle generated data such as:

- Oracle-generated related database files:
  - database datafile
  - control files
  - redo log files
  - archive log files
- Oracle-generated database backup files:
  - hot/cold
  - rman
  - datapump exports
- Oracle-generated database TDE local wallet files

> **Note**
> CTE on ACFS only provides encryption. It does not provide access control.

For other files such as manually created shell scripts that require staging in a shared storage device, use other shared storage setups such as Veritas shared storage or share NFS mount.

Oracle RAC
Oracle ACFS (File System)
Oracle ADVM (Volume Manager)
Oracle ASM (Storage Manager)
SecVM

On Oracle, ACFS is layered on ASM disks, which in turn are built on `secvm` block devices.

`secvm` is a proprietary device driver that supports GuardPoint protection to raw devices. `secvm` is inserted in between the device driver and the device itself.

DSM Security Administrators and SecVM

Server-side administrators must ensure that all `secvm` guards for an Oracle cluster use the same policies for encryption and access control.

Host Groups and Identical Keys and Policies

Thales recommends that you deploy host groups to ensure that identical policies and keys are applied on all nodes of the ACFS cluster. This is faster and less error-prone.

Restrictions and Caveats

- Thales does not support `secfs` layered on ACFS.
- Oracle ACFS encryption in conjunction with `secvm` encryption might impact performance

Oracle RAC ASM

This section describes how to install and configure CTE on an Oracle RAC ASM.

Using CTE with an Oracle RAC ASM

You can apply CTE when the Oracle DB is active or inactive. If you choose to use it while the Oracle DB is active, it eliminates any downtime. You can apply CTE during low volume traffic time frames. If you choose to use this option, then use the **rebalance** function of ASM. This allows you to:

1. Migrate data off of a disk so that it can be dropped/removed from a **Diskgroup**.
2. Apply CTE protection.
3. Add the disk back into the diskgroup.

> **CAUTION**
> **If you drop a disk from an ASM diskgroup, then add it back to the diskgroup without cleanly wiping the disk, the ASM diskname will be corrupted. To avoid this problem, clear out the disk before you add it back to diskgroup. Example:** `dd if=/dev/zero of=/dev/secvm/dev/mapper/asmdg-asmlv002 bs=32k`

Important ASM Commands and Concepts

Rebalancing Disks

When you drop/remove a disk from the diskgroup, it is important to apply the proper value for the power setting for rebalance and to use the `WAIT` command.

Example ASM Command:

```
SQL> ALTER DISKGROUP <DiskGroupName> DROP DISK <diskName> REBALANCE POWER 8 WAIT;
```

- The **`rebalance`** command moves the data off of the disk that you are removing from the diskgroup, distributing the data across the remaining DISKS.

- The **power** setting is a number from 1 to 11. It determines how much processing power is dedicated to the rebalance, versus normal operations. Unless the encrypting occurs during heavy traffic volume, the minimum value you should use is 6. Otherwise, consult the customer's DBA for the proper setting. An appropriate value to start with is 8.

Mapping Raw Devices

You can map raw devices for this configuration using:

- **EMC PowerPath**

  If using EMC PowerPath then the device names are similar to the following: `/dev/hdiskpowerXX`.

  When browsing the DSM through the local host, you cannot find Power Path devices. You must manually input the paths. The guarded disk names are prepended with: `/dev/secvm`.

Checking Rebalance Status

The `wait` command is very important when ASM performs a rebalance. When you specify `wait`, the command prompt does not display until all of the data is rebalanced and migrated off of the disk. If you do not specify wait, the command prompt returns immediately, and you must issue the following ASM command to check the status of the rebalance:

```
SQL> select * from v$asm_operation;
```

This command returns information about the:

- State
- Current power level
- Current amount rebalanced
- Estimated work until completion
- Rate
- Estimated minutes
- Any error codes

> **Note**
> It is highly recommended that you always specify the `wait` command when performing a **Drop Disk** with Rebalance. If it is not specified, ASM may prematurely release the disk, thereby allowing CTE to place a GuardPoint on the disk before the rebalance completes. This action may corrupt the data.

Oracle cautions against this issue:

> **CAUTION**
> **The `ALTER DISKGROUP...DROP DISK` statement returns before the drop and rebalance operations complete. Do not reuse, remove, or disconnect the dropped disk until the `HEADER_STATUS` column in the `V$ASM_DISK` view for this disk changes to `FORMER`. You can query the `V$ASM_OPERATION` view to determine the amount of time remaining for the drop/rebalance operation to complete. For more information, refer to the *Oracle Database SQL Language Reference* and the *Oracle Database Reference*.**

Determining Best Method for Encrypting Disks

A diskgroup can contain one or multiple disks. You must determine if the diskgroup contains enough disks and free space for encryption. If the diskgroup contains only one disk, or multiple disks but not enough free space, then you must use the **Offline** (backup/restore) method for encryption.

If the diskgroup contains more than one, you can use the **Online** (rebalancing) method. During rebalancing, additional disks allow for migrating data from the original disk so that it can be encrypted, added back into the diskgroup, and then migrated back to the source disk. Therefore, if the customer does not want to permanently add extra disks, they can add disks temporarily, just for rebalancing.

In general, once you have completed the initial setup for the operating system with which you are working, for both ASM or ASMLib, the high-level process is the same for applying CTE protection to raw devices and using them.

Online Method (No Application / Database Downtime)

Typically, when using the online method, follow these steps:

1. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
2. Apply CTE encryption to the disk.
3. Add each protected disk to the diskgroup.
4. Restart the nodes and the failover test.
5. Repeat the previous steps for each disk in the diskgroup.

Offline Method (Backup the DB)

Typically, when using the offline method, follow these steps:

1. Backup the database.
2. Make an ASM disk available for protection by either removing a disk from an existing diskgroup, or allocating a new disk.
3. Stop the Oracle database.
4. Delete the diskgroup.
5. Apply CTE encryption to the disk.
6. Recreate the diskgroup.
7. Add the protected disk to the diskgroup.
8. Restart the nodes and the failover test.
9. Repeat the previous steps for each disk in the diskgroup.

General Prerequisites

Setup

- Verify that you have a current backup of the database
- Install and register CTE agents on all RAC node Hosts
- Create a **Host Group** and add all RAC node hosts as members
- Create an encryption key for the Oracle RAC Database / Application
- Create an Oracle policy using the proper encryption key

> **Note**
> If the raw device mappings for the disk(s) are **not** identical across all nodes in the RAC, then you cannot use a Host Group for managing the GuardPoint within the DSM. You **must** apply the GuardPoint to each Host individually. This is typically not optimal, as a Host Group is the most effective and consistent way to manage GuardPoints for Oracle RAC environments.

Altering ASM_DISKSTRING on ASM

ASM uses the `asm_diskstring` setting to identify the path where ASM will attempt to locate available disks to use. If you are using device names when adding the disk, you must modify the string to include the path to SecVM.

1. To retrieve the `ASM_DISKSTRING` setting, type:

   ```
   SQL> SHOW PARAMETER ASM_DISKSTRING
   ```

2. To modify the setting, type:

   ```
   SQL> ALTER SYSTEM SET ASM_DISKSTRING='/dev/*', '/dev/secvm/dev/*';
   ```

   Where the path added is the path to SecVM.

Specific Prerequisites

Establishing a Starting Point

In many production environments, you may find that it has been a very long time since the RAC nodes have had the services restarted or have been completely rebooted. This can result in a lack of understanding of the actual state of the RAC cluster and its ability to survive a reboot on its own, prior to installing CTE.

Restarts can uncover issues in the RAC environment that are unrelated to CTE. To avoid issues after a CTE installation, Thales recommends that you restart each RAC node **AFTER** CTE is installed and **PRIOR** to establishing any GuardPoints. This may not be feasible in a single node configuration. However, by doing so, CTE is installed but inactive, and you can ensure that the platform is in a workable state prior to getting started.

The Importance of Device Mapping

It is important to use device naming and mapping in a multi-node RAC configuration. Verify the device names to ensure that the disks are mapped to the same disks on each RAC node before applying any GuardPoints. Thales recommends that RAC nodes use the same device names across all nodes. If they do not match, then problems can occur.

If the RAC nodes use the same device names, use a Host Group to create GuardPoints. If they do not match, do not use a Host Group to create GuardPoints. Set them up independently on each Host.

Important Note about Raw Devices on AIX

In general, raw devices are created as either character or block mode devices. Any I/O performed on character devices is non-buffered, while I/O on block devices is buffered and performed in defined block sizes (that is, 4K bytes).

While the Oracle documentation for using ASM with raw devices indicates that you can use either character or block devices, **CTE REQUIRES a block device for guarding**.

Notes

- Attempting to apply a GuardPoint on a character device that *does not* have a corresponding block device may result in a GuardPoint that never encrypts data. The status of the GuardPoint never shows as guarded.
- The WebUI does not support browsing for the character devices. You would need to manually paste the name into the WebUI.

Once guarded, CTE creates both a character and block mode version of the guarded device. Oracle ASM can use either device.

About Oracle RAC ASM Raw Devices

Standard Devices

In many cases the ASM configuration may be using plain device names, like the following:

```
/dev/hdisk1
```

Note
If you use standard device names in the ASM configuration to add a disk, you must modify the `ASM_DISKSTRING` parameter to include the `/dev/secvm/dev/*` path.

Consistent Naming of Devices across RAC Nodes

As previously stated, if the raw device mappings for the disk(s) are **NOT** identical across all nodes in the RAC, then you **CANNOT** use a Host Group and you **MUST** apply the GuardPoints to each Host individually. This is typically NOT optimal, as a Host Group is the most effective way to manage an Oracle RAC environment.

Oracle RAC ASM Multi-Disk Online Method

Performing encryption with the online rebalancing method requires sufficient free space to allow the drop of the largest ASM disk.

Checking for Space

In the Oracle system, use the following commands to check for available disk space:

1. Check total free space in the disk group:

```
SQL> SELECT name, free_mb, total_mb, free_mb/total_mb*100 as percentage FROM v$asm_
diskgroup;

NAME                             FREE_MB    TOTAL_MB PERCENTAGE
------------------------------ ---------- ---------- ----------
DATA                                    7       2109 .331910858
```

2. Check individual ASM disk size and usage:

```
SQL> select a.name DiskGroup, b.disk_number Disk#, b.name DiskName, b.total_mb, b.free_mb, b.path, b.header_status FROM v$asm_
disk b, v$asm_diskgroup a where a.group_number (+) =b.group_number order by b.group_number, b.disk_number, b.name

DISKGROUP  DISK#  DISKNAME        TOTAL_MB    FREE_MB   PATH                          HEADER_STATUS
---------  -----  --------       ---------    -------   ----------------------------  -------------
DATA         0    DATA_0000           1874       1273   /dev/oracleasm/disks/DATA3    MEMBER
DATA         1    DATA_0001           1992        608   /dev/oracleasm/disks/DATA4    MEMBER
DATA         3    DATA_0003            117          0   /dev/oracleasm/disks/DATA2    MEMBER
             0    DATA_ENC_0000        109         28   /dev/oracleasm/disks/DATA1_ENC  MEMBER
```

Adding a Disk to the Diskgroup

Using the Online Method assumes that there is enough free space in the diskgroup so that you can drop/remove a disk, protect it with CTE, and then add it back into the diskgroup.

To add the disk to the diskgroup:

1. Open a terminal session on both RAC Nodes.
2. On **RAC Node 1**, on the ASM, remove the disk from the disk group, type.

   ```
   SQL> ALTER DISKGROUP <diskGroupName> DROP DISK <diskName> REBALANCE POWER 11 WAIT;
   ```

3. On both **RAC Node 1** and **2** type:

   ```
   # chown oracle:oinstall /dev/<rawDevice1Name>
   # chmod 660 /dev/<rawDevice1Name>
   ```

4. On the DSM, in the Host Group, apply a GuardPoint to the Raw Device: <*rawDevice1Name*>.
5. From **RAC Node 1**, to display the status of the guarded disks, type:

   ```
   # secfsd -status guard
   ```

6. On both **RAC Node 1 and 2** type:

   ```
   # chown oracle:oinstall /dev/secvm/dev/<rawDevice1Name>
   # chmod 660 /dev/secvm/dev/<rawDevice1Name>
   ```

7. From **RAC Node, on the ASM,** add the protected disk to the disk group:

   ```
   SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDevice1Name> NAME
   <disk1Name>;
   ```

   The disk is now added to the diskgroup and ready for use.

8. The system is now ready for a reboot and failover test. For details, see "Surviving the Reboot and Failover Testing " on the next page.

Oracle RAC ASM Multi-Disk Offline Method (Backup/Restore)

Using the Offline Method assumes that there is not enough free space in the diskgroup.

1. Open a terminal session on both RAC Nodes.
2. On RAC Node 1, on the ASM, type the following to remove the disk group.

   ```
   SQL> DROP DISKGROUP <diskGroupName> FORCE INCLUDING CONTENTS;
   ```

   > **Note:** Make sure that the disk is removed before guarding the raw devices.

3. On both **RAC Node 1** and **2** type:

4. ```
   # chown oracle:oinstall /dev/<rawDevice1Name>
   # chmod 660 /dev/<rawDevice1Name>
   # chown oracle:oinstall /dev/<rawDevice2Name>
   # chmod 660 /dev/<rawDevice2Name>
   # chown oracle:oinstall /dev/<rawDevice3Name>
   # chmod 660 /dev/<rawDevice3Name>
   ```

5. On the DSM, in the Host Group, apply GuardPoints to the three raw devices:

   ```
   <rawDeviceName1>
   <rawDeviceName2>
   <rawDeviceName3>
   ```
   ```

6. On **RAC Node 1**, to display the status of the guarded disks, type:

   ```
   # secfsd -status guard
   ```

7. On both **RAC Node 1** and **2**, type:

   ```
   # chown oracle:oinstall /dev/secvm/dev/<rawDeviceName1>
   # chmod 660 /dev/secvm/dev/<rawDeviceName1>
   # chown oracle:oinstall /dev/secvm/dev/<rawDeviceName2>
   # chmod 660 /dev/secvm/dev/<rawDeviceName2>
   # chown oracle:oinstall /dev/secvm/dev/<rawDeviceName3>
   # chmod 660 /dev/secvm/dev/<rawDeviceName3>
   ```

8. From **RAC Node 1**, **on the ASM**, add the protected disk to the disk group, type:

   ```
   SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDeviceName1> NAME
   <diskName1>;
   SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDeviceName2> NAME
   <diskName2>;
   SQL> ALTER DISKGROUP <diskGroupName> ADD DISK /dev/secvm/dev/<rawDeviceName3> NAME
   <diskName3>;
   ```

   The disks are now added to the diskgroup and ready for use.

9. On **RAC Node 1**, restore the database.

10. The system is now ready for a reboot and failover test. Go to the section "Surviving the Reboot and Failover Testing " below.

Surviving the Reboot and Failover Testing

Failover Testing

Confirm that everything is functional:

- Ensure that the GuardPoints are all operational.
- Ensure that you receive valid results when you query the database.
- Verify that the load order ensures that CTE starts before ASM .

Once verified, you can start the failover testing for each RAC Node.

1. Reboot the RAC Node 1 and monitor the startup.
2. Once the restart is clean, reboot RAC Node 2 and monitor the startup.

Basic Troubleshooting Techniques

The following are some of the most common configuration issues that prevent the Oracle ASM configuration from working properly.

If you encountering errors similar to:

- ORA-15075: disk(s) are not visible cluster-wide
- ORA-15032: not all alterations performed

This could be the result of improper settings for the I/O layer, meaning that your disks are not properly configured.

Perform the following tasks to verify that the settings are correct:

1. On the DSM Management Console, in the Host Group that was created for the RAC cluster, verify that the host group for this configuration does **NOT** have the Cluster Group option set (this option is only for GPFS, which is not supported with CTE).
2. Ensure that the GuardPoints for the block devices are set at the Host Group level. This ensures that each node receives identical GuardPoints.
3. Verify that the GuardPoints are active on all nodes. When the GuardPoints are set, go to each node and verify that they are set and guarded, using the WebUI or the **`secfsd -status guard`** command. If they do not guard correctly, make sure the device names are the same across all nodes.
4. From ASM, make sure that the `asm_diskstring` parameter is modified to include the CTE devices and that the proper pathname is used, see "Altering ASM_DISKSTRING on ASM" on page 55.

Verifying Database Encryption

Option 1

The best way to verify the state of the data, without impacting anything in the existing environment, is to use the Oracle `kfed` command. You can run this command against the native path of the existing GuardPoints and make sure it returns with valid header information. If it returns valid information with the GuardPoint in place, then this confirms that the data is properly encrypted. If it returns with invalid header information, then that indicates that the data is either clear, double encrypted, or not in the expected encrypted state. The syntax for running this command would look similar to the following but will vary based on your environment.

```
# /app/oracle/grid/product/11.2.0/grid/bin/kfed read /dev/<diskName>
```

If the location is properly encrypted, following is an example of the viewable output:

```
# /app/oracle/grid/product/11.2.0/grid/bin/kfed read /dev/<diskName>
```

System Response:

```
    kfbh.endian:                          1 ; 0x000: 0x01
    kfbh.hard:                          242 ; 0x001: 0xf2
    kfbh.type:                          124 ; 0x002: *** Unknown Enum ***
    kfbh.datfmt:                         66 ; 0x003: 0x42
    kfbh.block.blk:              1088904227 ; 0x004: blk=1088904227
    kfbh.block.obj:              1558192170 ; 0x008: file=8234
    kfbh.check:                  3321251423 ; 0x00c: 0xc5f6465f
    kfbh.fcn.base:                932956641 ; 0x010: 0x379bc9e1
    kfbh.fcn.wrap:               3040493590 ; 0x014: 0xb53a4016
    kfbh.spare1:                 3806015223 ; 0x018: 0xe2db2ef7
    kfbh.spare2:                 3794962182 ; 0x01c: 0xe2328706
    60000000000D8000 01F27C42 40E75C23 5CE0202A C5F6465F
    [..|B@.\#\. *..F_]
    60000000000D8010 379BC9E1 B53A4016 E2DB2EF7 E2328706  [7....:@......2..]
    60000000000D8020 CA2F30AD 522B4D21 99292639 004EBB34  [./0.R+M!.)&9.N.4]
    60000000000D8030 A3896BE8 BD839D23 2204E19E 946C575C  [..k....#".....lW\]
    60000000000D8040 4CE2218F 35E1B101 AF751A70 780E6D6E  [L.!.5....u.px.mn]
    60000000000D8050 5E7E6A38 C600ED5F 929047C4 DF372A8E  [^~j8..._..G..7*.]
    60000000000D8060 E103152D BA87CC03 11A7D963 9D72FCE1
    [...-.......c.r..]
    60000000000D8070 1EC6B48B 03EE869F 61D651F9 E7614957  [........a.Q..aIW]
    60000000000D8080 810E0353 9C461F49 69569733 501D19EF  [...S.F.IiV.3P...]
    60000000000D8090 B268002B 4F9457B6 BDB04AC5 D3D07446  [.h.+O.W...J...tF]
    60000000000D80A0 FD9EE5E0 9B46CB66 30D10B22 F63AB77E  [.....F.f0.."0.:.~]
    60000000000D80B0 6FF79075 4BBD1FAD 8F226188 7774300D  [o..uK...."a.wt0.]
```

```
60000000000D80C0 A809B6FB E1F1C80B B5760E68 9747D97D  [.........v.h.G.}]
KFED-00322: Invalid content encountered during block traversal: [kfbtTraverseBlock][Invalid
OSM block type][][124]
```

Option 2

The second option to verify the state of the data is to use the `dd` command. This requires you to specify some blocks and write it out to a file. After this completes, read the file using the strings command. You can do this while the device is in use. In the example below some sectors are skipped and it only dumps 10000 counts.

For example:

```
# dd if=/dev/asm_data2p1 of=/tmp/dd2.out skip=1047 count=10000
```

Option 3

The third option to verify the state of the data without impacting the existing environment is to use the strings command.

> **Note**
> The strings command cannot read a busy or large device.

You can run this command against the native path (`/dev/<deviceName>`) of the existing GuardPoints (`/dev/secvm/dev/<deviceName>`). By executing the strings command against the native path **`strings /dev/devicename | more`**, this does not go through the SecVM device and therefore is not be decrypted. If it is encrypted the output should contain illegible text.

Chapter 5: Concise Logging

This chapter contains the following sections:

Overview of Concise Logging

Thales's standard operational logging sends audit messages for each file system operation. An audit message is sent 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.

Concise Logging allows you to focus on relevant audit messages and important actionable messages, such as errors and warnings. It can eliminate the repetitive and less important audit messages generated by read and write activity on a file, reading and writing directory attributes, and other file system activity.

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 DSM or CipherTrust Manager for the following:

- All registered hosts in all domains; see "Configuring Global Concise Logging with the DSM" on the next page.
- A host that has registered with the DSM; see "Configuring Concise Logging for a Registered Host with the DSM" on the next page.

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 host. CTE applies it to all GuardPoints and for all users on the host for which it is selected. There is no finer-grained control, such as per GuardPoint, user, or message type.
- When you enable this setting at the DSM level, it applies to all hosts in all domains, that are added to the DSM, but does not apply to any existing hosts. Hosts added after this setting is enabled inherit this setting. The default global setting is off.
- 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*.

Configuring Global Concise Logging with the DSM

You can enable or disable Concise Logging at any time. The DSM controls the function. Any change in the Concise Logging is reflected on any newly registered hosts and their domains.

To configure global Concise Logging:

1. Log in to the DSM with System Admin privileges.
2. Click **System > Log Preferences**. Your system may contain multiple log tabs.
3. Click on a **Log** tab.
4. In the Duplicate Message Suppression Settings field, click **Enable Concise Logging**.
5. Click **Apply**.
6. Repeat steps for any other logs, as appropriate.

   The host sends the following message after the administrator has enabled Concise Logging for an individual host:

   ```
   DAO00821: Administrator "voradmin" updated Security Server configuration "Concise Logging Enabled" from "true" to "false".
   ```

Configuring Concise Logging for a Registered Host with the DSM

You can enable Concise Logging for a host after you have registered it with the DSM. Hosts that are added to the DSM after enabling Concise Logging inherit the global settings from the DSM. This setting can be customized at any time.

To enable Concise Logging on the DSM for a registered host:

1. Log into your host with DSM Security Administrator privileges.
2. Select the host that you would like to customize.
3. Select a **Log** tab.
4. In the Duplicate Message Suppression Settings, click **Enable Concise Logging**.
5. Click **Apply**.

   After you enable or disable Concise Logging, CTE generates a log message to record that event:

   ```
   [CGA] [INFO] [CGA3201I] [11/11/2016 10:57:18] Concise logging enable
   [CGA] [INFO] [CGA3202I] [11/11/2016 10:57:27] Concise logging disabled
   ```

Chapter 6: Enhanced Encryption Mode

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

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.

	AES-CBC	AES-CBC-CS1
Security Improvements		
Unique IV per-file	No	Yes
IV predictability	Yes	No
File System Support		
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 DSM, 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.

  Notes
  - 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 DSM or 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 DSM

Deploy AES-CBC-CS1 encryption by using a symmetric agent key type created in the DSM:

1. In the DSM, click **Keys > Agent Keys > Keys**.
2. Click **Add**.
3. In the Encryption Mode dropdown, select **CBC-CS1**.
4. In the Algorithm dropdown, select **AES128** or **AES256** to create an AES-CBC-CS1 key.
5. Edit or create a policy that will use the AES-CBC-CS1 key. In this policy:
   - If you are using NFS, in the **Security Rules** section, add a security rule that specifies:

     Action: `f_rd_att`

     Effect: `Permit, Apply Key`

     This security rule allows CTE to read the base IV value in the file's embedded header over NFS. This rule is not needed if you are not using NFS.
   - In the **Key Selection Rules** section, click **Add** and select the AES-CBC-CS1 key.
6. Click **OK** to save the policy.
7. Push the policy to the GuardPoints that you want to use this encryption key.

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 Policies" chapter in the CTE Administrator Guide.

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.

Chapter 7: 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 chapter:

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 `secfsd` 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	
`-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

Command	Description
`-status policy`	list configured policies
`-status pslist`	list protected processes
`-status devmap`	list guarded devices
Manual GuardPoint options	
`-guard path [container ID]`	manually guard path
`-unguard path [container ID]`	manually unguard path
Version option	
`-version`	list version of kernel module `secfs2`

secfsd Examples

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.

Notes

- 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 or the DSM, 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
/bin/su 3E765375897E04C39AB17D4C755F50A35195535B6747DBA28DF9BD4AA672DFF9
|authenticator|/usr/sbin/sshd 98FC599D459EDEA52A60AB394B394803B5DAB96B53148DC608732DDA6777FA1A
/usr/sbin/in.rlogind 5C9A0EDD8BF54AE513F039476D21B3032507CF957AA0CB28C368EB8AB6E684FB
/bin/login 0D2EE0B995A30AE382B4B1CA5104715FC8902F457D283BDABAAD857B09259956
/usr/bin/gdm-binary 363780522E3CCF9ABF559F059E437743F9F97BBBB0EE85769007A464AD696BD1
/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.

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://vmSSA07:8444/upload/logupload, \
https://vmSSA05:8444/upload/logupload
Logger Certificate directory: /opt/vormetric/DataSecurityExpert/agent/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 DSM.

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: 7.0.0.11
```

Manually Enable a GuardPoint in DSM

To manually enable a GuardPoint on an AIX host:

1. Click **Hosts > Hosts > <*hostName*> GuardPoints**
2. Click **Guard**.
3. In the Policy field, select a policy.
4. Set Type to **Directory (Manual Guard)**.
5. Click **Browse** and enter the GuardPoint path.
6. Click **OK**.
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/etc
secfsd: 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
```

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/etc
secfsd: 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
```

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

`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

To display a CTE password challenge string and enter the response string when the DSM is not network accessible, use the `vmsec challenge` command. For example:

```
# vmsec challenge
Contact the help desk at 1-800-555-1212 for response generation.
Your host name is "Host120" Your challenge is: HPTQ-ZYLK
Response -> IHFY-W7WG-PDAO-QKKQ
```

The contact information is configured in the DSM Management Console (Domains > Manage Domains) *Add Domain* window. Contact the DSM Administrator and give them the challenge string. The DSM Administrator will give you the response string. Enter the response string in the **Response** field and press **Enter**. You have 15 minutes to enter the response string.

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=7.0.0.11
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,https://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.com: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=aes256
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
```

```
B92A3D7EEF67B82230F7F76097D65159FCF5722A4154A249EFDC22C20F1B572C
AUTHBIN_2=|authenticator|/bin/login
4F210D1B83ACD79B006BCF7DB247ED002A45FC892C42720390BFA6AE21AEA8DC
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) 2009-2020, 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=7.0.0
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
```

Binary Resigning

> **Note**
> The following issue applies to an existing VTE for AIX host registered with a DSM only. It does not apply to a CTE for AIX registered with CipherTrust Manager.

Prior to VTE for AIX version 5.2.7, any executable that is part of either a host setting or Signature Set, and that resides in a GuardPoint, will use a different signature for each key rotation. The result is that the host settings binaries will no longer be authenticated, or the Signature Set policy rules will no longer trigger for those binaries. To prevent these issues, the security administrator must manually resign each affected binary after each key rotation.

Starting with VTE for AIX version 5.2.7, CTE includes binaries that are signed with a signature that does not change with a key rotation. The security administrator must do only one manual resigning after the first key rotation. After that, there is no longer a need to resign after each subsequent key rotation.

If you are installing a CTE Agent for the first time, there are no special steps if no signatures have been defined. The CTE Agent will sign using the new method.

If you are upgrading or installing a new machine using the same signature sets that you used previously, do the following:

1. Install the latest version of the CTE Agent. The previous signatures will be used until the next key rotation.
2. Before the next key rotation, the administrator resigns the binaries.
3. Do not remove the old signatures on the DSM until all VTE Agents have been upgraded to CTE version 7.0.0.11. For information on how to do a manual resign, see the *DSM Administration Guide*.
4. When all agents have been upgraded, remove the old signatures.

> **Note**
> In previous versions, if the binary was in a GuardPoint protected directory, but was the same as an unguarded binary, the administrator could restrict to only the guarded binary. With this change, the unguarded binary is now unrestricted. This means that if a user uses the unguarded binary and its SHA matches the guarded binary, it will now match as if it was the guarded binary.

Enable Automatic Signing for Host Settings

CTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software based on the assumption that restarting the `vmd` will generate new signatures when signed software is updated. This process will not work with CTE unless you disable automatic signing.

To disable automatic signing:

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:
   ```
   RE_SIGN_HOST_SETTINGS=TRUE
   ```
4. Save your changes and exit the file.
5. Restart the vmd to set the changes, type: `# /etc/vormetric/secfs restart`
6. Type the following to verify that the host settings is set to true:
   ```
   # vmsec vmdconfig
   ```

> **WARNING**
> **Enabling the automatic regeneration of signatures exposes a potential security vulnerability for agents. When enabled, host setting binaries are resigned when it receives a push from the DSM. If an attacker were to replace a binary with a Trojan, and then force a push from the DSM by, for example, restarting the agent, CTE could generate a signature for the malicious binary and pass it to the kernel.**

Restricting Access Overrides from Unauthorized Identities

In some setups, system administrators can use the host settings > |authenticator| feature with `su` to change identities and gain access to restricted data. You can instruct CTE to not trust any authentication attempt performed by certain identities by assigning restricted users to a user shell that CTE 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.

CTE 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.

To restrict access overrides in **DSM**:

1. In the DSM Management Console, click **Hosts > Hosts**.
2. Click on an existing Host name to edit the host.
3. Click **Host Settings** tab.
4. Add the following to the host 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 **OK**.

To restrict access overrides in **CM**:

1. In the CM dashboard, click **CTE > 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**.

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
7.0.0.11
2020-09-20 11:09:40 (IST)
Copyright (c) 2009-2020, Thales.. All rights reserved.
```

agenthealth Utility

The `agenthealth` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to DSM 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
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
security.manager.com is resolvable ..............  OK
security.manager.com port 8446 is reachable ......  OK
security.manager.com port 8447 is reachable ......  OK
security.manager.com is resolvable ..............  OK
security.manager.com port 8446 is reachable ......  OK
security.manager.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..................  2020-082-13 20:25:37.446
Checking available disk space....................  OK
Checking logging space ..........................  OK
                Log directory is "/var/log/vormetric"
                File system for log data is "/", 32G free (17% full)
                Log directory contains 2 of maximum 200 files (1% full)
```

```
                Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to /ofx-fs1 ..................... OK
Testing access to /gp1 ........................... Access denied as per policy
```

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 DSM 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
```

-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

register_host Utility

Use the `register_host` utility to create certificate requests, exchange certificates between the DSM and the host, and to register CTE on the DSM. 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 DSM 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.

Chapter 8: Upgrading CTE on AIX

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

> **Note**
> Currently, you can only upgrade a VTE for AIX host to CTE version 7.0.0.11 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.

This chapter contains the following sections:

Upgrading the VTE Agent Interactively

This section describes the generic instructions for upgrading a VTE Agent to a CTE Agent. For specific instructions, refer to the *Release Notes* for the agent.

You can also configure CTE to perform the upgrade the next time the server restarts. For details, see "Scheduling a CTE Agent Upgrade" on the next page.

To upgrade the VTE Agent interactively:

1. Stop any application accessing files in the GuardPoint.
2. Log on to the host where you will upgrade CTE. You must have root access.
3. Copy or mount the installation file onto the host system.
4. Start the upgrade by executing the install program for the release to which you want to upgrade.

   For example, the following command upgrades the product to version 7.0.0.11:

   ```
   # ./vee-fs-7.0.0-11-aix71.bin
   ```
5. Type **Y** and press Enter at the prompt to accept the CTE License Agreement. The upgrade proceeds.
6. Follow the prompts. During an upgrade, the following message displays. Enter **Y** at the prompt:

   ```
   Upgrade detected: this product will be stopped and restarted.
   Do you wish to proceed with the upgrade? (Y/N) [Y]: Y
   Installation success.
   ```

   You will not do the registration steps since the host is already registered with the DSM.

   > **Note:** You must continue to use the DSM as your key manager after the upgrade. You cannot upgrade a VTE Agent to CTE and then change the registration to use CipherTrust Manager.
7. To verify that the upgrade was successful, use the `vmd -v` command:

   ```
   $ vmd -v
   Version 7
   7.0.0.11
   2020-09-20  09:45:20 (IST)
   Copyright (c) 2009-2020, Thales. All rights reserved.
   ```

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.

> **Notes**
> - 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 7.0.0.11.
> - Currently, you can only upgrade a VTE for AIX host to CTE version 7.0.0.11 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.

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.
- DSM 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.
- You must continue to use the DSM as your key manager after the upgrade. You cannot upgrade a VTE Agent to CTE and then change the registration to use CipherTrust Manager.

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-7.0.0-11-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-7.0.0-11-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.

Chapter 9: 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.