

CipherTrust Transparent Encryption

CTE Agent for DSM

Linux Quick Start Guide

Release: 7.5.0

Document Version 1

December 19, 2023



CipherTrust Transparent Encryption

CTE Agent for DSM

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries and affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2009-2023 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Contents

Preface	3
Audience	3
The CTE Agent Documentation Set	3
Document Conventions	3
Typographical Conventions	3
Notes, Tips, Cautions, and Warnings	3
Chapter 1: Overview of CTE	5
CTE Terminology	5
CTE Components	5
How to Protect Data with CTE	6
Chapter 2: Configuring CTE for Linux with a DSM	7
Installation Overview	7
Installation Prerequisites	7
Recommendations and Considerations	7
Network Setup Requirements	7
Port Configuration Requirements	8
Communication with Key Manager	8
Communication for LDT over CIFS/NFS	8
CTE Registration Method Options	8
Installing and Registering CTE	8
Installing CTE and Registering Using the Shared Secret Registration Method	9
Installing CTE and Registering Using the Certificate Fingerprint	12
Guarding a Device with the DSM	16
Access the DSM Domain	16
Create an Encryption Key	16
Create a Standard Policy	16
Create a GuardPoint	17
Caveats	17
Prerequisites	17
Procedure	17

Preface

Audience

The *CTE Agent for DSM* is intended for system administrators who install and configure CipherTrust Transparent Encryption (CTE) on Linux.

The CTE Agent Documentation Set

The CTE for DSM guides are available at: [CTE for DSM Documentation Site](#).

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 2-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options	Click the System tab and select General Preferences .
<i>bold italic monospaced font</i>	Variables or text to be replaced	https://< <i>Token Server name</i> >/admin/ Enter password: < <i>Password</i> >
regular monospacedfont	<ul style="list-style-type: none">• Commands and code examples• XML examples	session start iptarget=192.168.253.102
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	<i>/usr/bin/</i>
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>CTE Agent for DSM</i> for information about CipherTrust Transparent Encryption.
quotes	<ul style="list-style-type: none">• File extensions• Attribute values• Terms 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.

Chapter 1: Overview of CTE

This document describes how to install CipherTrust Transparent Encryption (CTE) to protect data on physical or virtual machines.

CTE protects data at rest, residing on Direct Attached Storage (DAS), Network Attached Storage (NAS) or Storage Area Networks (SAN). This can be a mapped drive or mounted disk, as well as through Universal Naming Convention paths.

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

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	<p>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.</p> <div style="border: 1px solid black; padding: 5px;"><p>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 <code>/opt/vormetric/DataSecurityExpert/agent/</code>.</p></div>
CTE Agent	<p>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.</p>
key manager	<p>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.</p>
host / client	<p>In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.</p> <p>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.</p>
GuardPoint	<p>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.</p>

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 that supports most CTE for Linux features.
- The *Vormetric Data Security Manager (DSM)*, Thales's legacy key manager that supports all CTE for Linux features.

Both key managers can be set up as either a security-hardened physical appliance or a virtual appliance. Both provide access to the protected hosts through a browser-based, graphical user interface as well as an API and a CLI.

Thales recommends that you use the CipherTrust Manager unless you need a feature that is only supported by the DSM, as described below.

- Container Security
- CTE-IDT

For details about any of these features, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* and *CTE-Live Data Transformation with Data Security 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 [CTE Compatibility Portal](#) or the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)

How to Protect Data with CTE

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

Policies specify:

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

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

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

Chapter 2: Configuring CTE for Linux with a DSM

This chapter describes how to install CTE on a Linux system using the standard, interactive installation script, then register that system with a Vormetric Data Security Manager (DSM) and use the DSM to create a standard GuardPoint on the Linux host.

If you want to register CTE with a CipherTrust Manager, see [Chapter 1: "Configuring CTE for Linux with CipherTrust Manager" on page 1](#).

This section contains the following topics:

Installation Overview	7
Installation Prerequisites	7
Installing and Registering CTE	8
Guarding a Device with the DSM	16

Installation Overview

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

1. Set up your systems according to the requirements of the selected key manager.
2. Create your policies, encryption keys, and GuardPoints using the selected key manager.

Installation Prerequisites

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

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0 or later will fail.
- 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-7.5.0.78-rh8-x86_64.bin -d /home/hello/
```

- Ensure read/write permission is granted to other users accessing your shared resource.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity between the DSM and the host on which you install CTE. Ideally, there should be a two-way communication flow between the DSM and the host.
- If the host is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

Communication with Key Manager

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

Communication for LDT over CIFS/NFS

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

- 7024
- 7025

CTE Registration Method Options

Before you can install CTE, you need to select a registration method. You can register the protected hosts with a DSM using either the *Fingerprint method* or the *Shared Secret method*.

- **Fingerprint method** requires the 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 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 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 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.

Installing and Registering CTE

Thales provides a standard interactive installation script that asks you a series of questions during the install. The script prompts you to register CTE with a key manager immediately after the installation has finished. CTE must be registered with a key manager before you can protect any of the devices on the host.

The procedure for installing CTE and registering it with a DSM depends on the registration method you want to use. The available methods are described in "[CTE Registration Method Options](#)" above. 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 the facing page
- "[Installing CTE and Registering Using the Certificate Fingerprint](#)" on page 12

Note

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

Installing CTE and Registering Using the Shared Secret Registration Method

The following procedure describes how to install the CTE Agent on the Linux host and then register the CTE Agent with a DSM using the Shared Secret registration method. For Fingerprint registration, see ["Installing CTE and Registering Using the Certificate Fingerprint" on page 12](#).

Prerequisites

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-7.5.0.78-rh8-x86_64.bin
```

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

```
# ./vee-fs-7.5.0.78-rh8-x86_64.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-7.5.0.78-rh8-x86_64.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: 7.5.0.78
```

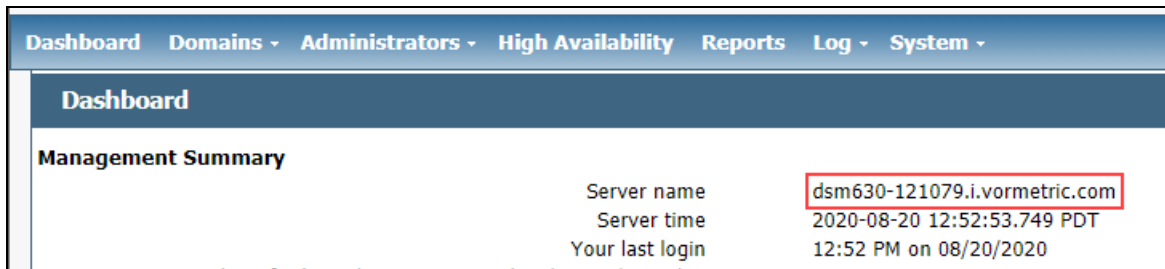
In order to register the CipherTrust Transparent Encryption File System Agent with a Vormetric Data Security Manager

- 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 Key Manager you need a valid registration token from the CM.

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

5. Enter **y** to continue with the registration process. The install script prompts you to enter the 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-RHEL-14.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**

- At this point, the install script asks you about some of the optional CTE features you may want to enable, such as CTE-IDT, CTE-LDT, and docker support.

Note: Some of these features may require a separate license in the DSM.

For example:

```
Do you want this host to have docker support enabled on the server? (Y/N) [N]:
```

```
Do you want this host to have Efficient Storage support enabled on the server?  
(Y/N) [N]:
```

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]:
```

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

Note: You can only install the Cloud Object Storage feature during installation. You cannot install it post installation.

- 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.
```

- 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 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 Shared Secret registration, see ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 9](#).

Prerequisites

Make sure that the Administrator has added 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-7.5.0.78-rh8-x86_64.bin
```

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

```
# ./vee-fs-7.5.0.78-rh8-x86_64.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-7.5.0.78-rh8-x86_64.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: 7.5.0.78
```

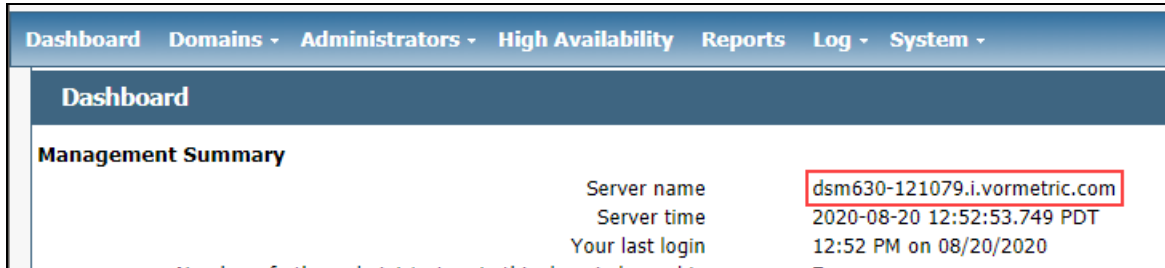
```
In order to register the CipherTrust Transparent Encryption File System Agent
with a Vormetric Data Security Manager
```

- 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 Key Manager you need a valid registration
token from the CM.
```

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

5. Enter **y** to continue with the registration process. The install script prompts you to enter the 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-RHEL-14.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
```

- At this point, the install script asks you about some of the optional CTE features you may want to enable, such as CTE-IDT, CTE-LDT, and docker support.

Note: Some of these features may require a separate license in the DSM.

For example:

```
Do you want this host to have docker support enabled on the server? (Y/N) [N]:
```

```
Do you want this host to have Efficient Storage support enabled on the server?  
(Y/N) [N]:
```

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]:
```

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

Note: You can only install the Cloud Object Storage feature during installation. You cannot install it post installation.

- 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.
```

- Verify with the 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.
- 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 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 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**.

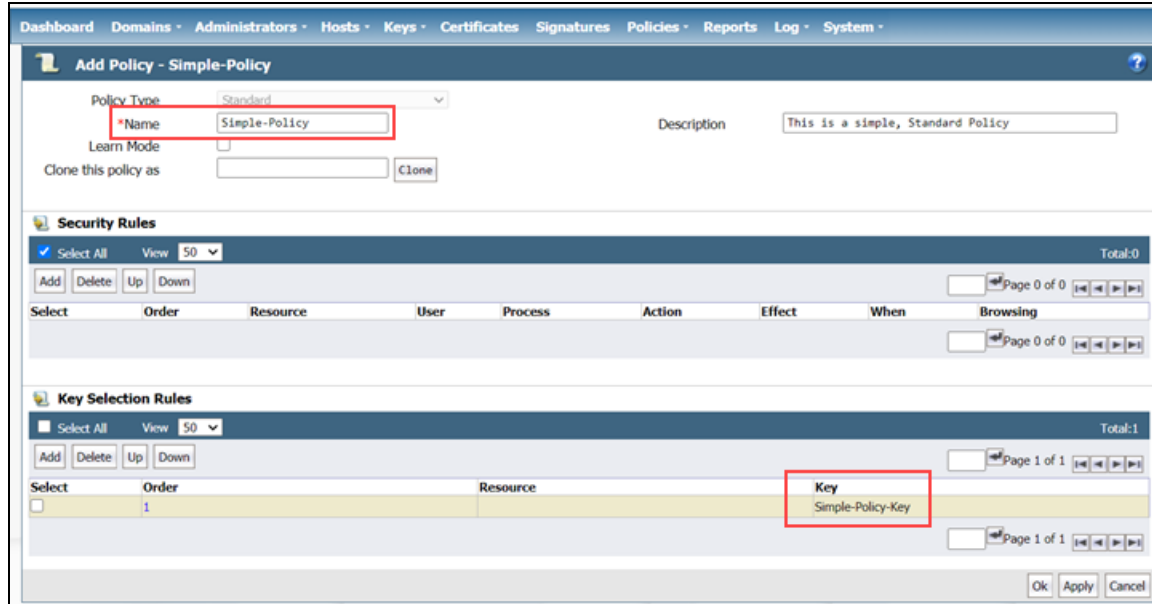
Create an Encryption Key

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

Caveats

- You cannot have a symlink reside inside of a GuardPoint that is pointing to another location in that same GuardPoint
- You cannot have a symlink reside inside of a GuardPoint that points to the root of that same GuardPoint

Prerequisites

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

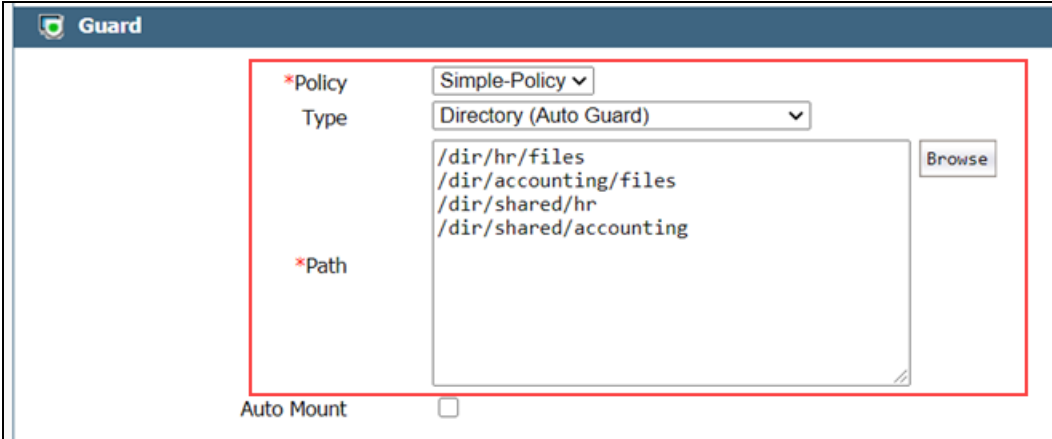
Note

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

Procedure

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



The screenshot shows a window titled "Guard" with a blue header. The main area contains several fields: a dropdown menu for "Policy" set to "Simple-Policy", a dropdown menu for "Type" set to "Directory (Auto Guard)", a text area for "Path" containing four lines of directory paths: "/dir/hr/files", "/dir/accounting/files", "/dir/shared/hr", and "/dir/shared/accounting". To the right of the text area is a "Browse" button. At the bottom left, there is an "Auto Mount" checkbox which is currently unchecked.

- d. Click **Ok**.
- The DSM pushes the GuardPoint configuration to the host.
6. Type the following to transform the data:

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

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

THALES

Contact us

For office locations and contact information,
visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

