THALES

CipherTrust Transparent Encryption

CTE Agent for DSM

Windows Quick Start Guide

Release 7.3.0

Document Version 1

November 22, 2022

CTE Agent for DSM
November 22, 2022

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.

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.

Contents

Preface ..... **iii**

Audience iii

The CTE Agent Documentation Set iii

Document Conventions iii

- Typographical Conventions iii
- Notes, Tips, Cautions, and Warnings iii

Chapter 1: Overview of CTE ..... **v**

CTE Terminology v

CTE Components vi

How to Protect Data with CTE vi

Chapter 2: Configuring CTE for Windows with a DSM ..... **viii**

Installation Overview viii

Installation Prerequisites viii

- CTE Registration Method Options viii
- Network Setup Requirements viii
- Host Name Resolution Requirements ix
- Port Configuration Requirements ix

Installing and Registering CTE ix

- Installing CTE and Registering Using the Shared Secret Registration Method x
- Installing CTE and Registering Using the Certificate Fingerprint Method xii

Guarding a Device with the DSM xiv

- Access the DSM Domain xv
- Create an Encryption Key xv
- Create a Standard Policy xv
- Create a GuardPoint xvi
  - Caveats xvi
  - Prerequisites xvi
  - Procedure xvi

Preface

Audience

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

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 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`	- Commands and code examples - XML examples	`session start iptarget=192.168.253.102`
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 DSM* for information about CipherTrust Transparent Encryption.
quotes	- 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	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 C:\Program Files\Vormetric\DataSecurityExpert\agent\. For example, the default installation directory is /opt/vormetric/DataSecurityExpert/agent/ for Linux and AIX, and C:\Program Files\Vormetric\DataSecurityExpert\agent\ for Windows.
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.
key manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. 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 that supports most CTE for Windows features that supports most CTE features on Linux and Windows, and all CTE features on AIX.
  - The *Vormetric Data Security Manager* (DSM), Thales's legacy key manager that supports all CTE for Windows featuresthat supports all CTE features on Linux, Windows, and AIX.

  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 though 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-Efficient Storage

  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 Windows with a DSM

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

If you want to register CTE with a CipherTrust Manager, see Chapter 1: "Configuring CTE for Windows with CipherTrust Manager" on page 1.

This section contains the following topics:

Installation Overview viii

Installation Prerequisites viii

Installing and Registering CTE ix

Guarding a Device with the DSM xiv

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.

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.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the Windows system on which you plan to install CTE to the CipherTrust Manager. After the Windows system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.

- It must also allow for connectivity of the CipherTrust Manager to all clients where you install CTE as well as communication between different CTE clients that need to communicate.
- If the system 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 DSMCipherTrust Manager and protected hosts. If you use FQDNs, your protected hosts must be able to resolve the DSMCipherTrust Manager host names, and the DSMCipherTrust Manager 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 DSMCipherTrust Manager and hosts.

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

- Use the IP addresses of the DSMCipherTrust Manager and protected hosts.
- Add an entry for the DSMCipherTrust Manager in the `C:\WINDOWS\system32\drivers\etc\hosts` file on each one of the Windows machines on which you want to install the CTE Agent.
- Add an entry in the `/etc/hosts` file on the DSMCipherTrust Manager associated with the host. The administrator must use the CipherTrust CLI, and, in an HA environment, they must add an entry to *each* DSMCipherTrust Manager in the cluster because entries in the `/etc/hosts` file are not replicated across the cluster.

Port Configuration Requirements

If a protected hostclient must communicate with the DSMCipherTrust Manager through a firewall, see the *DSM Administration Guide*CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

The default port for communication between the DSMCipherTrust 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.

Installing and Registering CTE

Thales provides a standard InstallShield installer that asks you a series of questions during the install. The installer 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" on the previous page. 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 Method" on page xii

> **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 host and then register the CTE Agent with a DSM using the Shared Secret registration method. For information about the Fingerprint registration method, see "Installing CTE and Registering Using the Certificate Fingerprint Method" on page xii.

Prerequisites

Make sure you know the following information from the Administrator:

- The server name of the primary DSMCipherTrust Manager .
- The shared secret for the domain on the primary DSMCipherTrust Manager with which you want to register the host.
- The name of the domain in the DSMCipherTrust Manager with which you want to register the host.
- Optionally, the name of the host group in which this host should be included.
- The registration token for the DSMCipherTrust Manager.

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

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

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the *License Agreement* page, accept the License Agreement and click **Next**.
6. On the *Live Data Transformation for network shares* page:
   - On this server, do you plan to protect CIFS/SMB-based GuardPoints with Live Data Transformation (LDT) add on? If so, select **yes**.
   - Select **No** if you:
     - Are using a DSM.
     - Plan to create local file system GuardPoints with standard and LDT policies on this host.
     - Apply GuardPoints on local CIFS shares using standard or LDT policies.

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

7. On the *Destination Folder* page, click **Next** to accept the default folder or click **Change** to select a different folder. When you are done, click **Next**.

   > **Notes**
   >
   > - Thales recommends that you install CTE in the default installation directory, `C:\Program Files\Vormetric\DataSecurityExpert\agent\`
   > - You must install the CTE Agent on the same drive as Windows. For example, if Windows is installed on the `C:` drive, you must install the CTE Agent on the `C:` drive.

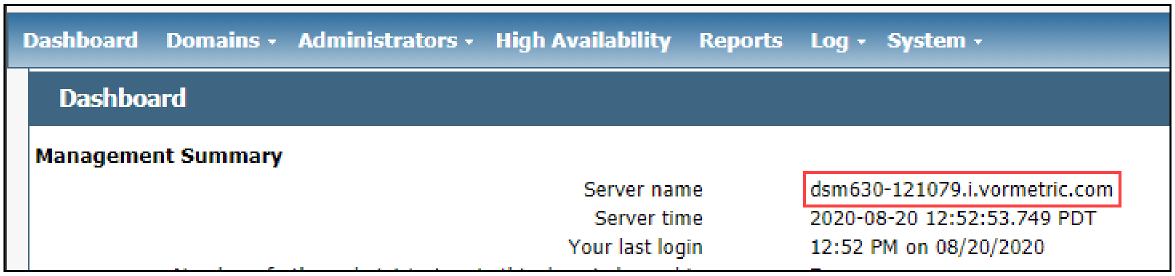
8. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.

9. On the *InstallShield Wizard Completed* page, make sure the **Register CipherTrust Transparent Encryption now** check box is selected and click **Finish**. The installer opens the Register Host wizard.

10. In the Register Host dialog box, verify the host's machine name and click **Next**.

11. On the *Gathering agent information* page, select the **File System** check box and click **Next**.

12. On the *Gathering Key Manager information* page, enter the FQDN of the Primary DSM. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.

    Dashboard

    Management Summary

    Server name dsm630-121079.i.vormetric.com
    Server time 2020-08-20 12:52:53.749 PDT
    Your last login 12:52 PM on 08/20/2020

    When you are done, click **Next**. CTE communicates with the selected DSM to validate what features have been licensed and are available to the CTE Agent.

13. On the *Gathering host name information* page:

    - Specify the host name or IP address of the host. You can select the host name from the drop-down list or type it in the field. If you specify a host name, it must be resolvable by the DNS server.
    - To enable cloning prevention, select the **Enable Hardware Association** check box.
    - If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the host, select the **Enable LDT Feature** check box. For details on CTE-LDT, see the *CTE-Live Data Transformation with Data Security Manager*.
    - If you want to have the CTE-Efficient Storage feature available on the host, select the **Enable ES Feature** check box. For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
    - Make sure the **Use Shared Secret Registration** check box is enabled.

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

    > **Note:** If you get the message “Only CTE-initiated communication is possible”, make sure that the DSM and CTE can communicate over the network.

14. On the *Gathering shared secret registration information* page, enter the following:
    - **Shared secret**:The shared secret established for the domain in the DSM to which you intend to add this host. Contact the Administrator for this value.
    - **Domain name**: The name of the DSM domain to which the host will be added. Contact the Administrator for this information.
    - **Host group** (optional): The name of the host group to which the host will be added. Contact the Administrator for this value.
    - **Host description** (optional): A user-defined description of the host to be registered.

    > ⚠ **WARNING**
    > **The shared secret, domain name, and host group are case-sensitive. If any of these are entered incorrectly, an error message displays. If you exceed the number of allowable login attempts to the DSM, you will be locked out of the DSM. For more information, talk to your Administrator.**

    When you are done, click **Register**. CTE contacts the DSM and attempts to register the host with the specified options. The Register Host dialog box displays a message with the results of the registration request.

    If the registration completed successfully, click **Finish**.

15. Restart the host to complete the installation process.

16. After the host has rebooted, you can verify the installation by checking CTE processes:
    a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
    b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.

Installing CTE and Registering Using the Certificate Fingerprint Method

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 Shared Secret registration method, see "Installing CTE and Registering Using the Shared Secret Registration Method" on page x.

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 DSMCipherTrust Manager and CTE can communicate with each other over the network.

Procedure

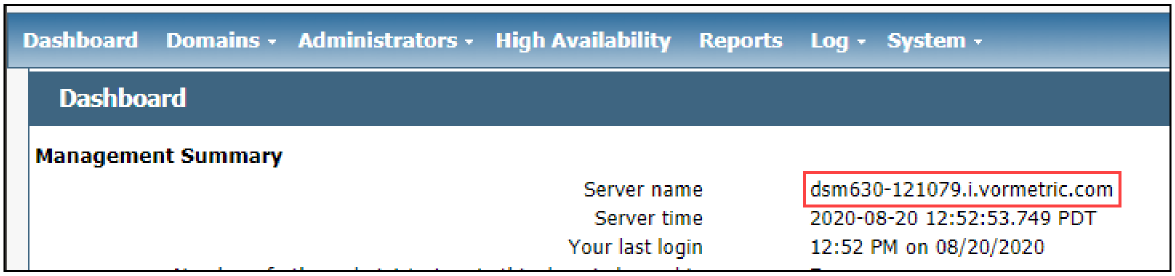
On the *InstallShield Wizard Completed* page, make sure the **Register CipherTrust Transparent Encryption now** check box is selected and click **Finish**. The installer opens the Register Host wizard.

In the Register Host dialog box, verify the host's machine name and click **Next**.

> **Note:** The machine name shown here does *not* need to match the one specified in the DSM. You will have an opportunity to select a different machine name later in this procedure.

On the *Gathering agent information* page, select the **File System** check box and click **Next**.

On the *Gathering Key Manager information* page, enter the FQDN of the Primary DSM. This name must match the name shown in the **Server name** field in the **Management Summary** section on the DSM **Dashboard** page.



Management Summary

Server name dsm630-121079.i.vormetric.com
Server time 2020-08-20 12:52:53.749 PDT
Your last login 12:52 PM on 08/20/2020

When you are done, click **Next**. CTE communicates with the selected DSM to validate what features have been licensed and are available to the CTE Agent.

On the *Gathering host name information* page:

- Specify the host name or IP address of the host. You can select the host name from the drop-down list or type it in the field. If you specify a host name, it must be resolvable by the DNS server.

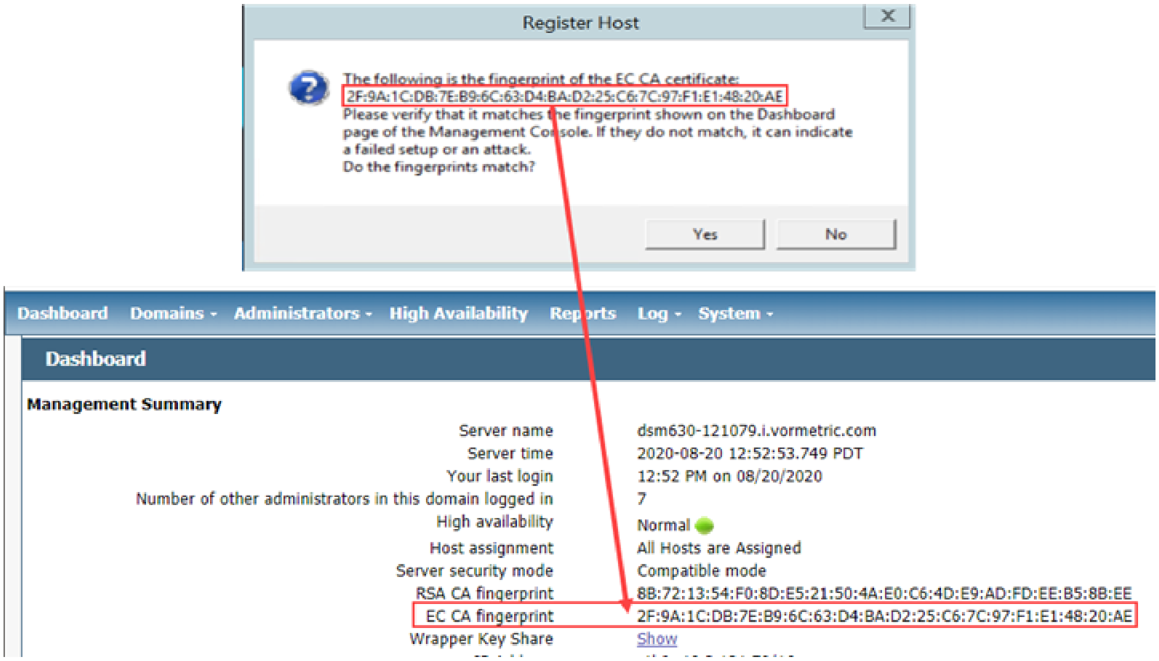
  WARNING
  The host name specified here must exactly match the host name specified in the DSM in order for the fingerprints to match.

- To enable cloning prevention, select the **Enable Hardware Association** check box.
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the host, select the **Enable LDT Feature** check box. For details on CTE-LDT, see the *CTE-Live Data Transformation with Data Security Manager*.
- If you want to have the CTE-Efficient Storage feature available on the host, select the **Enable ES Feature** check box. For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
- Clear the **Use Shared Secret Registration** check box so that CTE will use the Fingerprint Registration Method.

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

> **Note:** If you get the message “Only CTE-initiated communication is possible”, make sure that the DSM and CTE can communicate over the network.

CTE displays the Register host status page and displays the EC CA Certificate that it received from the DSM. This fingerpring should exactly match the fingerprint displayed on the DSM Dashboard page. For example:



The following is the fingerprint of the EC CA certificate:
2F:9A:1C:DB:7E:B9:6C:63:D4:BA:D2:25:C6:7C:97:F1:E1:48:20:AE
Please verify that it matches the fingerprint shown on the Dashboard page of the Management Console. If they do not match, it can indicate a failed setup or an attack.
Do the fingerprints match?

Management Summary

Server name	dsm630-121079.i.vormetric.com
Server time	2020-08-20 12:52:53.749 PDT
Your last login	12:52 PM on 08/20/2020
Number of other administrators in this domain logged in	7
High availability	Normal ●
Host assignment	All Hosts are Assigned
Server security mode	Compatible mode
RSA CA fingerprint	8B:72:13:54:F0:8D:E5:21:50:4A:E0:C6:4D:E9:AD:FD:EE:B5:8B:EE
EC CA fingerprint	2F:9A:1C:DB:7E:B9:6C:63:D4:BA:D2:25:C6:7C:97:F1:E1:48:20:AE
Wrapper Key Share	Show

If the fingerprints match, click **Yes**.

Click **OK** when CTE displays the fingerprint for the host's certificate.

The *Register host status* page shows the two fingerprints and displays a message about the registration status. If the registration completed successfully, click **Finish**.

Restart the host to complete the installation process.

After the host has rebooted, you can verify the installation by checking CTE processes:

1. In the system tray of the protected host, right-click the CipherTrust Lock icon.
2. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.

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**.

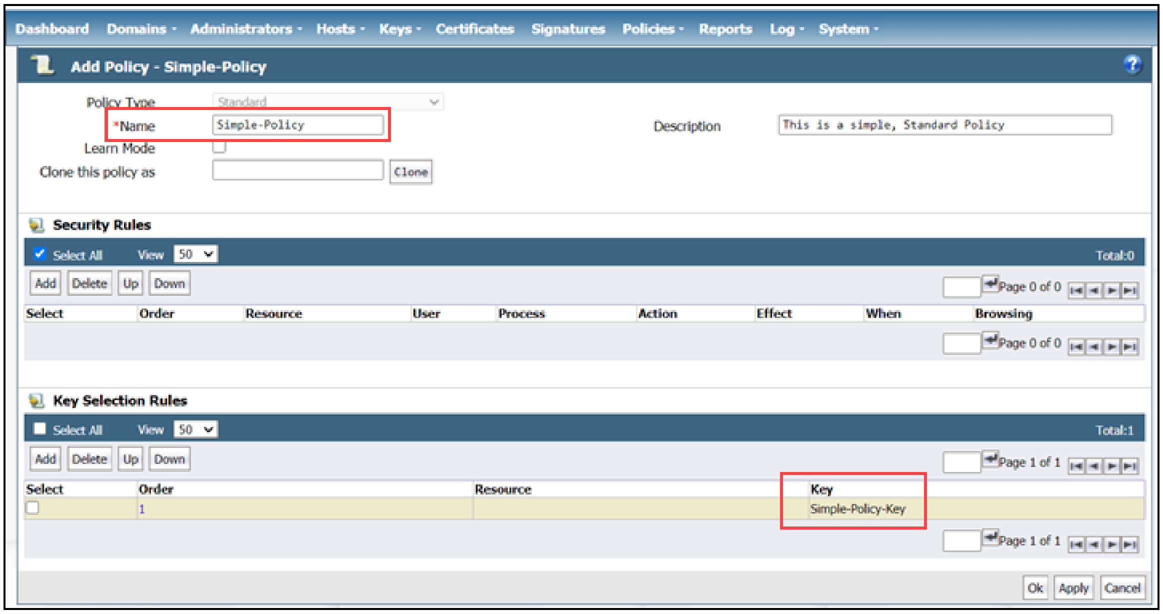
Create an Encryption Key

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**.



Policy Type: Standard
*Name: Simple-Policy
Learn Mode □
Clone this policy as: Clone
Description: This is a simple, Standard Policy

Security Rules

Select	Order	Resource	User	Process	Action	Effect	When	Browsing

Key Selection Rules

Select	Order	Resource	Key
□	1		Simple-Policy-Key

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.

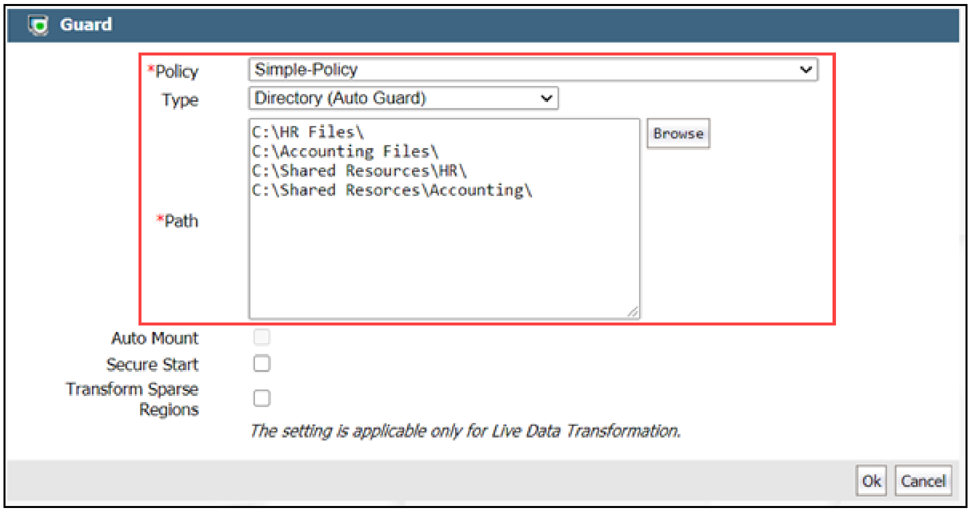
- C:\HR Files\
- C:\Accounting Files\
- C:\Shared Resources\HR\
- C:\Shared Resources\Accounting\

> **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:



Guard

*Policy: Simple-Policy

Type: Directory (Auto Guard)

*Path:

```
C:\HR Files\
C:\Accounting Files\
C:\Shared Resources\HR\
C:\Shared Resorces\Accounting\
```

Auto Mount □

Secure Start □

Transform Sparse Regions □

The setting is applicable only for Live Data Transformation.

   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 <