THALES

CipherTrust Transparent Encryption

CTE Agent for Windows Quick Start Guide

Release 7.1.0

CTE Agent for Windows Quick Start Guide
7.1.0
Document Version 1
March 23, 2021

Contents

Preface

Audience

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

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 Data Transformation 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 7.1.0.66*

- *Release Notes for CTE for Windows Version 7.1.0.66*

- *Release Notes for CTE for AIX Version 7.1.0.26*

To access any of these guides for the latest releases of CTE Agent, go to https://thalesdocs.com/ctp/cte/index.html.

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**.

Table 3-1: Typographical Conventions (continued)

Convention	Usage	Example
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 Windows Quick Start Guide* 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.**

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/encryption/contact-us
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

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.

  CipherTrust Manager versions 2.2 and higher support all CTE for Windows features *except* for the following:

  - CTE-Efficient Storage. (For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.)

  - CTE-Live Data Transformation over CIFS shares, (For details about using CTE-LDT with CIFS, see the *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 CTE documentation is available at https://thalesdocs.com/ctp/cte/index.html.

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: Installation Overview

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 and support different features, so you must make this decision first. For details, see "CTE Components" on page 8.

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

   - Chapter 3: "Configuring CTE for Windows with CipherTrust Manager" on page 11
   - Chapter 4: "Configuring CTE for Windows with a DSM" on page 20

3. Create your policies, encryption keys, and GuardPoints using the selected key manager. For an example, see one of the following:

   - "Guarding a Device with CipherTrust Manager" on page 14.
   - "Guarding a Device with the DSM" on page 26.

> **Note**
> This document describes only the basic installation options for an interactive install. For additional options, such as the procedures for a silent installation, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.

Chapter 3: Configuring CTE for Windows with CipherTrust Manager

This chapter describes how to install CTE on a Windows system using the standard, interactive installer, then register that system with CipherTrust Manager and use CipherTrust Manager to create a standard GuardPoint on the Windows client.

If you want to register CTE with a Vormetric Data Security Manager (DSM), see Chapter 4: "Configuring CTE for Windows with a DSM" on page 20.

This chapter contains the following topics:

Installation Prerequisites

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

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.

- 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.

Installing and Registering CTE

The Windows interactive install uses a standard InstallShield wizard that asks you a series of questions during the installation. 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.

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a CipherTrust Manager. If you want to install CTE and register it with a Vormetric Data Security Manager, see Chapter 4: "Configuring CTE for Windows with a DSM" on page 20.

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 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:

   - Select **Yes** if you plan to use CTE-LDT with CIFS share GuardPoints on this host. If you select **Yes**, you will *not* be able to guard any local directories on this host, even if those directories use a Standard CTE policy. Only CTE-LDT GuardPoints on CIFS shares will be supported for this host.

   - Select **No** if you only plan to create local file system GuardPoints on this host. If you select **No**, you will *not* be able to use CTE-LDT with any CIFS share GuardPoints on this host.

     > **Note:** If you intend to register this host with CipherTrust Manager, make sure you select **No**. Creating CTE-LDT GuardPoints on a CIFS share is not currently supported with CipherTrust Manager. This functionality will be supported in a future release.

   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 or IP address of the primary CipherTrust Manager.

    When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager 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 client. You can select the host name from the drop-down list or type it in the field.

    - 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 client, select the **Enable LDT Feature** check box. For details on CTE-LDT, see *CTE-Live Data Transformation with CipherTrust Manager*.

    When you are done, click Next.

14. On the *Gathering registration information* page, enter the following:

    - **Registration token**:The registration token for the CipherTrust Manager with which you want to register this host.

    - **Profile name**: The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.

    - **Host group** (optional): The name of the client group to which the client will be added.

    - **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.

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

    When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client 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 client to complete the installation process on the client.

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.

    - If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.

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

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" below. If you need to change to a different domain, do the following:

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

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

    c. The logged in user now shows the new domain name/user name.
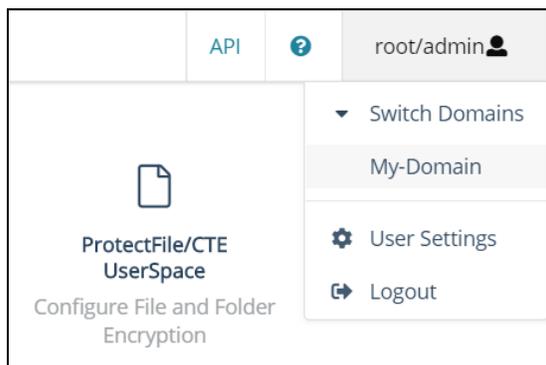
Create an Encryption Key

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

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

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

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

3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.

4. In the **Key Usage** section, make sure **Encrypt** and **Decrypt** are selected.

5. Click **Create**. CipherTrust Manager displays the properties for the new key.

6. In the general options area, enable the **Exportable** option.

   You can also enable the **Deletable** option in this section if you want a CipherTrust Manager Administrator to be able to delete the key.

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

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

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

   b. Click the **All** check box for both the CTE Admins and CTE Clients groups.

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

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

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

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

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

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

     When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.

   - **Encryption Mode**: Encryption mode of the key. The options are:

     - CBC
     - CBC CS1
     - XTS

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

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

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.

2. In the sidebar on the Clients page, click **Policies**.

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

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

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a **Standard** policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/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.

Field	Description
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 14.

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:

   - `C:\HR Files\`

   - `C:\Accounting Files\`

   - `C:\Shared Resources\HR\`

   - `C:\Shared Resorces\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 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:
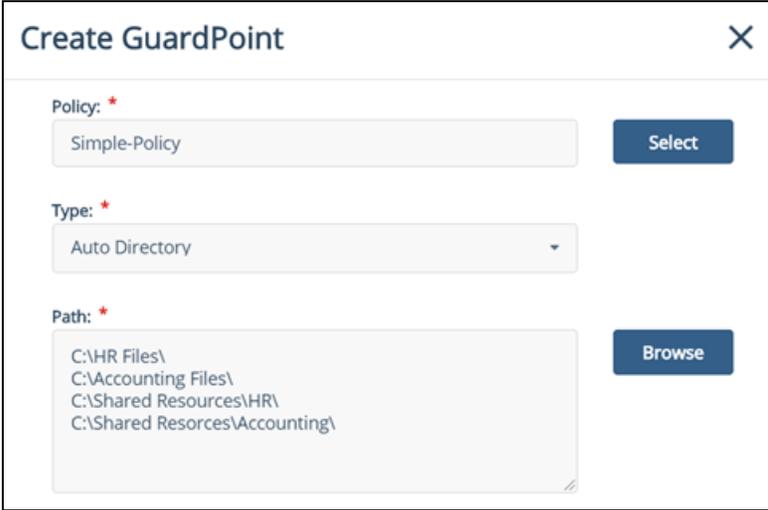
   d. Click **Create**.

   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.

Chapter 4: 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 3: "Configuring CTE for Windows with CipherTrust Manager" on page 11.

This chapter contains the following topics:

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 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.

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.

- 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 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 for the DSM 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 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.

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" below

- "Installing CTE and Registering Using the Certificate Fingerprint Method" on page 24

> **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 24.

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 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:

   - Select **Yes** if you plan to use CTE-LDT with CIFS share GuardPoints on this host. If you select **Yes**, you will *not* be able to guard any local directories on this host, even if those directories use a Standard CTE policy. Only CTE-LDT GuardPoints on CIFS shares will be supported for this host.

   - Select **No** if you only plan to create local file system GuardPoints on this host. If you select **No**, you will *not* be able to use CTE-LDT with any CIFS share GuardPoints on this host.

   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.

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 DSM Administrator for this value.

- **Domain name**: The name of the DSM domain to which the host will be added. Contact the DSM Administrator for this information.

- **Host group** (optional): The name of the host group to which the host will be added. Contact the DSM 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 DSM 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 21.

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

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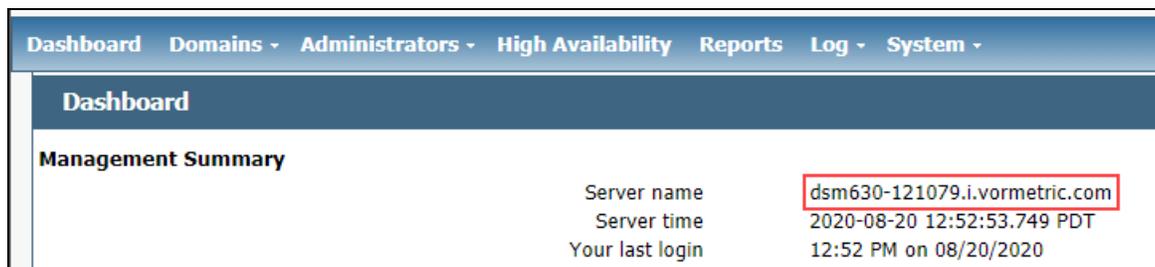
When you are done, click **Next**. CTE communicates with the selected DSM to validate what features have been licensed and are available to the CTE Agent.

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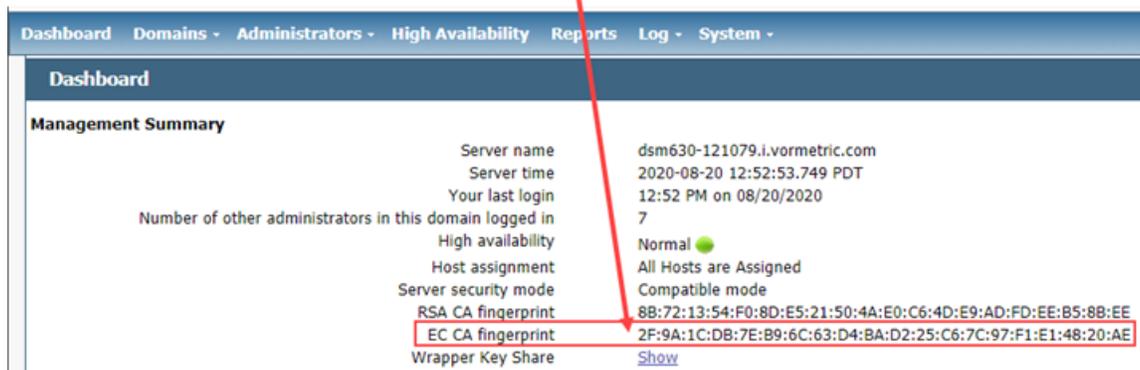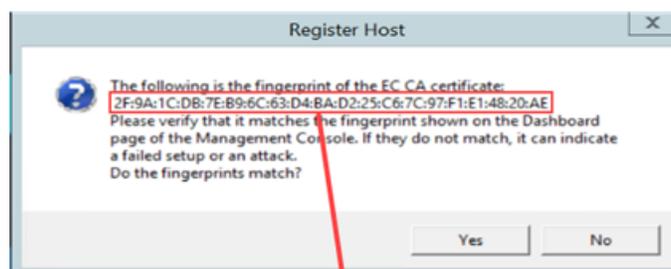
If the fingerprints match, click **Yes**.

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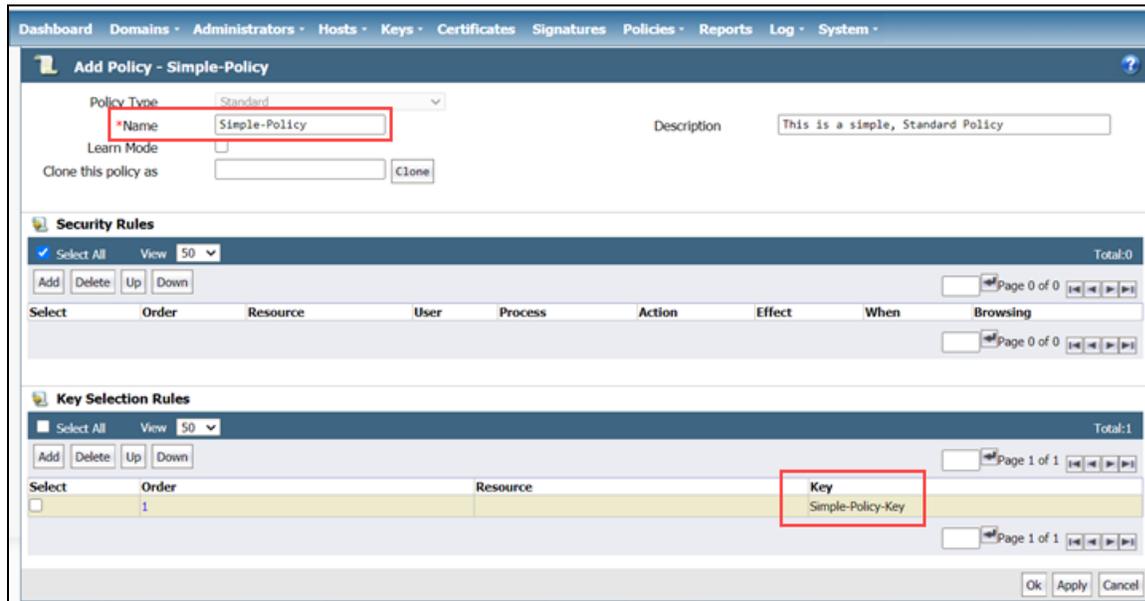
4. Click **Ok** to create the policy.

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:

   - `C:\HR Files\`
   - `C:\Accounting Files\`
   - `C:\Shared Resources\HR\`
   - `C:\Shared Resorces\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:
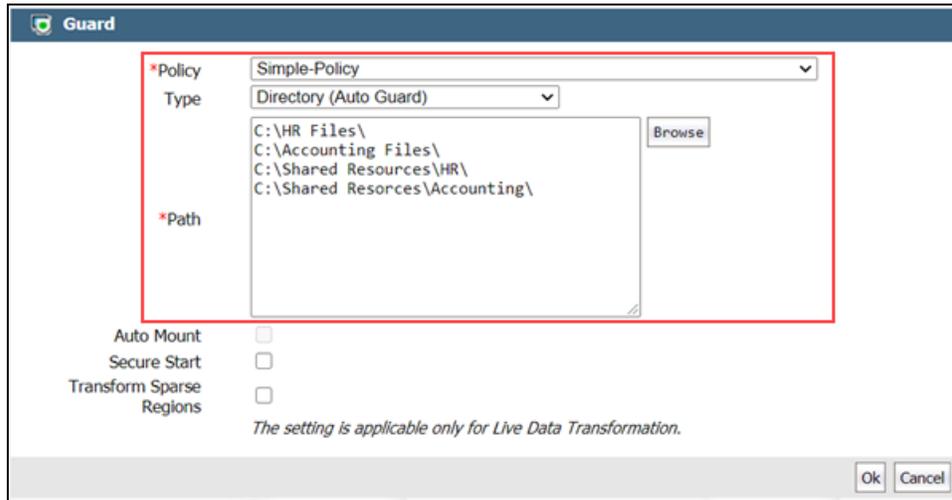
    d. Click **Ok**.

    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.

THALES

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

> cpl.thalesgroup.com <