

THALES

CTE Terminology

CTE V7.6.0



CTE Terminology

The guide 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> <p>Note: This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric".</p> <p>For example, the default installation directory is <code>/opt/vormetric/DataSecurityExpert/agent/</code> for Linux and AIX, and <code>C:\Program Files\Vormetric\DataSecurityExpert\agent\</code> for Windows.</p>
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 CipherTrust Manager - a key manager for use with CTE.</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>
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 CipherTrust Manager, next generation key manager that supports most CTE for Linux and Windows features, most CTE features on Linux and Windows, and all CTE features on AIX.

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

CipherTrust Manager versions support all CTE for Linux features *except* for the following:

- Container Security

Support for these features will be included in future releases of the CipherTrust Manager.

CipherTrust Manager versions 2.7 and higher support all CTE for Windows features *except* for the following:

Support Contacts

If you encounter a problem while installing, registering, or operating the product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at [Thales Customer Support](#), is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

Tip

You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@Thales.com.