

CipherTrust Transparent Encryption

CTE Agent for Windows for DSM

Advanced Configuration and Integration Guide

Release: 7.5.0

Documentation Version 1

December 19, 2023



CipherTrust Transparent Encryption

CTE Agent for Windows for DSM

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

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

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

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

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

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

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

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

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

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

Contents

Preface	9
The CTE Agent Documentation Set	9
Document Conventions	9
Typographical Conventions	9
Notes, Tips, Cautions, and Warnings	9
Chapter 1: Overview of CTE	11
CTE Terminology	11
CTE Components	12
How to Protect Data with CTE	12
Chapter 2: Getting Started with CTE for Windows	14
Installation Workflow	14
Installing CTE with No Key Manager Registration	14
Configuring CTE for Windows with a DSM	16
Assumptions	16
Requirements	16
Installation and Registration Options and Prerequisites	16
Installation Method Options	16
CTE Registration Method Options	16
Host Name Resolution Requirements	17
Port Configuration Requirements	17
Communication with Key Manager	17
Communication for LDT over CIFS/NFS	17
One-way Communication Option	18
Hardware Association (Cloning Prevention) Option	18
CTE Windows Installation Checklist	18
Interactive Installation on Windows	19
Installing CTE and Registering Using the Shared Secret Registration Method	20
Installing CTE and Registering Using the Certificate Fingerprint Method	22
Silent Installation on Windows	24
Silent Installation Using the exe File and Shared Secret Registration Method	25
Silent Installation Using the MSI File and Shared Secret Registration Method	28
Silent Installation Using the exe File and Fingerprint Registration Method	31
Silent Installation Using the MSI File and Fingerprint Registration Method	34
All Windows Silent Install Command Line Options	37
Registering CTE with the Shared Secret Registration Method After Installation is Complete	40
Registering CTE with the Fingerprint Registration Method After Installation is Complete	42

Guarding a Device with the DSM	45
Access the DSM Domain	45
Create an Encryption Key	45
Create a Standard Policy	46
Create a GuardPoint	46
Chapter 3: Special Cases for CTE Policies	48
More Information About Configuring CTE Policies	48
Re-Signing Executable Files on Secfs GuardPoints	48
Re-Enabling Automatic Signing for Host Settings	49
Behavior of Hard Links Inside and Outside of GuardPoints (Windows)	49
Chapter 4: Enhanced Encryption Mode	50
Compatibility	50
Difference between AES-CBC and AES-CBC-CS1	50
Disk Space	51
Encryption Migration	51
File Systems Compatibility	51
Storing Metadata	51
Missing IV file	52
FileTable Support on Windows	52
Using the AES-CBC-CS1 Encryption Mode in DSM	52
Exceptions and Caveats	53
Best Practices for AES-CBC CS1 Keys and Host Groups	53
Chapter 5: Utilities for CTE Management	54
voradmin secfs Commands	54
voradmin secfs List Commands	54
voradmin secfs status Commands	55
vmsec Utility	56
vmsec Syntax	56
Displaying the CTE Challenge String	56
Using the CTE Challenge String	57
agenthealth Utility	57
Agent Health Check Script	57
agentinfo Utility	58
agentinfo Utility (Java version)	58
agentinfo Utility (PowerShell version)	58
PowerShell version agentinfo parameters	58

Examples for using agentinfo utility (PowerShell version)	59
Backup Utility	59
Agent is installed in the default location	59
Using a backup image to install to other agents or restore to a different system	59
Performing a backup while the agent is running	60

Chapter 6: Using CTE with Microsoft SQL **61**

Using CTE with SQL	61
Using LDT with SQL FILESTREAM	61
Using CTE with SQL FileTables	61
Considerations	61
Advantages	62
Supported FileTables Use Cases	62
CTE Data Transformation of existing files in FileTables	62
Protect files in SQL FileTables with CTE	62
Protect files with SQL AlwaysOn Availability Groups with CTE	63
Install CTE on remote systems and guard the SQL Server VNN names	63
Unsupported FileTables Use Cases	63
Installing CTE on Microsoft SQL AlwaysOn	63
Methods for Initial Encryption	64
Configuration 1	64
Configuration 2	64
Configuration 3	65
Configuration 4	66
Configuration 5	66
Data Transformation (Encryption in place)	67
Copy/Restore	67
SQL Server Policy Tuning	67
Using LDT with SQL AlwaysOn	67

Chapter 7: CTE with DFSR **68**

Overview	68
CTE Encryption Methods	68
Considerations with DFSR	69
CTE Configuration Workflow	70
Creating Required DFSR Policy Components	70
Using the Standard Encryption Method	74
Creating Standard Policies for DFSR	75
Creating Standard GuardPoints with the DFSR Hub and Spoke Topology	80

Creating Standard GuardPoints with the DFSR Full Mesh Topology	83
Using the CTE-LDT Encryption Method	84
Creating a CTE-LDT Policy for DFSR	85
Creating a CTE-LDT GuardPoint for DFSR	87
Chapter 8: Secure Start	89
Secure Start Overview	89
Prerequisites	89
Encrypt by Moving the AD Service into a Guarded Directory	90
Create the AD GuardPath directory	90
Apply Secure Start GuardPoints to a Directory with the DSM	90
Apply Secure Start GuardPoints to a Directory with CipherTrust Manager	90
Verify the Secure Start GuardPoint with CLI	91
Move the AD Database into the Secure Start GuardPoint	91
Encrypt Data in Place with Offline Transformation	91
Encrypt with an LDT Transformation Policy	92
Configure the Time Out Failure	92
Recover a Server After it Loses Connection to the Key Manager	93
DSRM Mode	93
Other Use Cases	93
Boot a Windows Server in Azure	94
Best Practices for Encrypting and Protecting the AD Service	94
Access Control with Secure Start	94
Creating a Minimal Policy Required for AD with Access Control	94
Creating a Restricted Policy in DSRM Mode	95
Guard Directories	96
Perform Subsequent System State Backups	96
Chapter 9: Exchange DAG	97
Exchange DAG Overview	97
Supported Use Cases for CTE in an Exchange DAG Environment	97
Unsupported Use Cases	98
Requirements for Exchange DAG Encryption	98
CTE Policies for Exchange DAG	99
Creating a Policy for CTE-LDT Encryption with CipherTrust Manager	99
Creating Policies for Standard Encryption with CipherTrust Manager	100
Creating the Initial Encryption Policy	101
Creating the Production Policy	102
Creating a Policy for CTE-LDT Encryption with the DSM	103

Creating Policies for Standard Encryption with the DSM	103
Creating the Initial Encryption Policy	104
Creating the Production Encryption Policy	105
Encrypting with CTE-LDT in an Exchange DAG Environment	105
Encrypting with a Standard CTE Policy in the Exchange DAG Environment	108
Decrypting with CTE-LDT in an Exchange DAG Environment	110
Chapter 10: Storage Spaces Direct	112
S2D Overview	112
Deployment Options	112
Supported Use Cases	113
Chapter 11: Using CTE with Quantum StorNext	114
Overview of using CTE with Quantum StorNext	114
CTE and Quantum StorNext Compatibility	114
Supported StorNext Server and Client Configurations	114
Supported GuardPoint and Key Settings for SNFS File Systems	115
Supported Concurrent Access Read/Write Scenarios	115
Setting up CTE and Quantum StorNext Integration	116
Integration Task Overview	116
Installing and Configuring a Quantum StorNext MDC Server for Use with CTE	117
Installing and configuring Quantum StorNext DLC Clients for Use with CTE	117
Choosing a Mounting Method	117
Installing the CTE Agent on Each StorNext LAN client	117
Chapter 12: Upgrading CTE on Windows	119
To Upgrade in Windows Silently	119
Verify the Windows Installation	119
Resolving Problems that Prevent Silent Install	119
CTE Scheduled Upgrade	120
Scheduling a CTE Upgrade on the Command Line	120
Scheduling a CTE Upgrade Interactively (self-extracting .exe only)	120
Show Scheduled CTE Upgrades	121
Cancel a Scheduled CTE Upgrade	121
Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades	121
Finding The Name Used For A Previous MSI Installation or Upgrade	122
MSI File Name Lookup Method 1: PowerShell	122
MSI File Name Lookup Method 2: Windows Registry	122

Chapter 13: Uninstalling CTE from Windows	123
Considerations	123
Procedure	123
 Appendix A: Troubleshooting and Best Practices	 124

Preface

The he CTE for DSM guides are available at: [CTE for DSM Documentation Site](#). CTE Agent for Windows for DSM provides information about advanced installation, configuration, and integration options for CTE for Windows.

The CTE Agent Documentation Set

T

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 .
<i>bold italic monospaced font</i>	Variables or text to be replaced	https://< <i>Token Server name</i> >/admin/ Enter password: < <i>Password</i> >
regular monospacedfont	<ul style="list-style-type: none">• Commands and code examples• XML examples	session start iptarget=192.168.253.102
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	<i>/usr/bin/</i>
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>CTE Agent for Windows for DSM</i> for information about CipherTrust Transparent Encryption.
quotes	<ul style="list-style-type: none">• File extensions• Attribute values• Terms used in special senses	"js", ".ext" "true" "false", "0" "1+1" hot standby failover

Notes, Tips, Cautions, and Warnings

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

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

Note

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

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

Tip

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

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



CAUTION

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

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



WARNING

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

Chapter 1: Overview of CTE

For very large data sets, initial encryption deployments can affect data availability, require unacceptable maintenance windows or require cloning and synchronizing data. Encrypting millions of files can span hours or even days, which can delay encryption, or require extra disk space and data synchronization, which can be labor-intensive. Rekeying large data sets can demand significant processing time and lengthy maintenance windows. Security and IT teams face tough tradeoffs, having to choose between security and availability.

CipherTrust Transparent Encryption operates with minimal disruption, effort, and cost. Its transparent approach enables security organizations to implement encryption without changing application, networking, or storage architectures. CipherTrust Live Data Transformation builds on these advantages, offering patented capabilities that deliver breakthroughs in availability, resiliency and efficiency.

CTE includes several unique utilities to help you encrypt and manage your data. It also integrates with several third-party platforms such as Oracle, Microsoft SQL, and Quantum StorNext.

This document describes the installation and advanced configuration options for CTE, as well as detailed information about how to integrate CTE with the supported third-party products.

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	<p>CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect.</p> <div style="border: 1px solid black; padding: 5px;"><p>Note</p><p>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 C:\Program Files\Vormetric\DataSecurityExpert\agent\.</p></div>
CTE Agent	<p>The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.</p>
key manager	<p>An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers two key managers for use with CTE, the Vormetric Data Security Manager (DSM) and CipherTrust Manager.</p>
host / client	<p>In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.</p> <p>The difference comes from the key manager you are using. The DSM refers to the machines as hosts, while the CipherTrust Manager refers to them as clients.</p>
GuardPoint	<p>A device or directory to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.</p>

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.
After the CTE Agent has encrypted a device on a host, that device is called a *GuardPoint*. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.
- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Thales offers two key managers that work with CTE:

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

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

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

- Container Security
- CTE-IDT

For details about any of these features, see the *CTE Agent for Linux Advanced Configuration and Integration Guide* and *CTE-Live Data Transformation with Data Security Manager*.

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

Note

For a list of CTE versions and supported operating systems, see the [CTE Compatibility Portal](#) or the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

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

How to Protect Data with CTE

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

Policies specify:

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

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

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

Chapter 2: Getting Started with CTE for Windows

This chapter describes how to install CTE for Windows, register it with your selected key manager, and then create a simple GuardPoint on the protected host. It contains the following topics:

Installation Workflow	14
Installing CTE with No Key Manager Registration	14
Configuring CTE for Windows with a DSM	16

Installation Workflow

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

1. Select which key manager you want to use. The Vormetric Data Security Manager and the CipherTrust Manager have different requirements and support different features, so you must make this decision first. For details, see ["CTE Components" on page 12](#).
2. If you want to install the CTE Agent without registering with a key manager, see ["Installing CTE with No Key Manager Registration" below](#). However, you cannot protect any data on the host until it has been registered. Otherwise, set up your systems according to the requirements of the selected key manager. For details, see one of the following:
 - ["Configuring CTE for Windows with a DSM" on page 16](#).
3. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see one of the following:
 - ["Guarding a Device with the DSM" on page 45](#).

Installing CTE with No Key Manager Registration

The following procedure installs the CTE Agent on the host but does not register it with a key manager. You cannot protect any data on the host until the CTE Agent is registered with one of the supported key managers. For a comparison of the available key managers, see ["CTE Components" on page 12](#).

If you want to register the CTE Agent immediately after installing it, see [Chapter 1: "Configuring CTE for Windows with CipherTrust Manager" on page 1](#) or ["Configuring CTE for Windows with a DSM" on page 16](#).

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 *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.

7. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. To tell the installer that you want to register later, clear the check box for **Register CipherTrust File System now**, then click **Finish**.
9. Reboot the host system to complete the installation.

Configuring CTE for Windows with a DSM

This section describes how to install and configure CTE on Windows computers and, optionally, registering CTE with a Vormetric Data Security Manager (DSM). If you want to register CTE with a CipherTrust Manager, see [Chapter 1: "Configuring CTE for Windows with CipherTrust Manager" on page 1](#).

The installation and configuration process consists of three basic steps:

1. Gather the information needed for the install and set up your network as described in ["Installation and Registration Options and Prerequisites" below](#).
2. Install CTE on the protected host as described in ["Interactive Installation on Windows" on page 19](#) or ["Silent Installation on Windows" on page 24](#).
3. Register the protected host with the primary DSM and make sure that the CTE Agent and the DSM can communicate with each other. Registration can be done as part of the initial installation or at any point after the CTE Agent has been installed.

Assumptions

- The IP addresses, routing configurations, and DNS addresses allow connectivity between the key manager and all hosts on which the CTE Agent is installed.
- If the protected host is a virtual machine, the VM is deployed and running.

Requirements

- You must install CTE on the system drive. Do *not* install CTE on a network share volume.
- The host on which you want to install CTE *must* support AES-NI hardware encryption.

Installation and Registration Options and Prerequisites

CTE has the following installation prerequisites and provides the following installation and registration options. The options you choose determine the information you need to supply during the actual install procedure, so you should decide what options you want to use before you start the installation.

Installation Method Options

There are two methods for installing CTE:

- **Interactive installation:** This is the most common and recommended type of installation. Use this for installing CTE on one host at a time using a standard InstallShield installation and registration wizard. See ["Interactive Installation on Windows" on page 19](#).
- **Silent installation:** Create pre-packaged installations by providing information and answers to the installation questions. Use silent installations when installing on a large number of hosts. See ["Silent Installation on Windows" on page 24](#).

CTE Registration Method Options

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

- **Fingerprint method** requires the 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.

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.

Port Configuration Requirements

Communication with Key Manager

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

Communication for LDT over CIFS/NFS

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

- 7024
- 7025

One-way Communication Option

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

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

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

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

Port Usage in One-Way Communications Mode

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

Hardware Association (Cloning Prevention) Option

CTE's hardware association feature associates the installation of CTE with the machine's hardware. When enabled, hardware association prohibits cloned or copied versions of CTE from contacting the key manager and acquiring cryptographic keys. Hardware association works on both virtual machines and hardware hosts.

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

To verify if hardware association (cloning prevention) is enabled on the protected host, access the Windows command line and run the `vmsec.exe hwok` command. The default location of `vmsec.exe` is `C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin`.

To change the status from enable to disable or vice versa:

1. Open the system tray and right-click on the CipherTrust Lock icon.
2. Select **Register Host**.
3. Follow the prompts to re-register CTE with the DSM.
4. Select **Enable hardware association** in the wizard.

CTE Windows Installation Checklist

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

Checklist item	Status
Get the CTE installation binary from Thales support, either self-extracting .exe file or MSI. The format for the self-extracting executable CTE file name is: vee-fs-<release>-<build>-<system>.exe Example: vee-fs-7.5.0-78-win64.exe The format for MSI CTE file name is: vee-<agent_type-build-system>.msi For example: vee-fs-7.5.0-78-win64.msi	
Get the Fully Qualified Domain Name (FQDN) of the DSM.	
Determine the Administrator password for the host.	
Determine if you want to do an interactive (InstallShield) or silent (command line) install.	
Determine if you want to register the CTE Agent with the DSM using the Shared Secret registration method or the Fingerprint registration method. For more information, see "CTE Registration Method Options" on page 16 .	
If using Shared Secret registration, obtain the following from the Administrator: <ul style="list-style-type: none"> • Shared secret for the DSM. • The Domain in which this host should be registered. • (Optional) Host Group in which this host should be added. 	
If using the Fingerprint registration, ask the Administrator to add the host to the DSM with the Registration Allowed check box selected. After you verify the fingerprints, the Administrator can select the Communication Enabled check box.	
Decide if you want to enable cloning prevention as described in "Hardware Association (Cloning Prevention) Option" on the previous page .	
Determine if you will register the IP address or the FQDN of the client. If you want to use the FQDN, make sure that there is a communication channel between the client and the DSM as described in "Host Name Resolution Requirements" on page 17 .	
Decide if your environment will only support client-initiated communication as described in "One-way Communication Option" on the previous page . <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Note: Thales recommends that you only use this option if your environment will not allow two-way communication between the CTE Agent and the CipherTrust Manager. </div>	
Open the appropriate ports as described in "Port Configuration Requirements" on page 17 . The default CTE Agent port is 7024 for two-way communication.	
Synchronize host clock to DSM clock.	

Interactive Installation on Windows

The Windows typical install uses an interactive InstallShield wizard that asks you a series of questions during the installation. You can also install CTE using a silent installer which pre-packages the install information. This allows you to install CTE on a large number of hosts. (For more information, see ["Silent Installation on Windows" on page 24](#)).

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

The procedure for installing CTE depends on the registration method you want to use. The available methods are described in ["CTE Registration Method Options" on page 16](#). 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 22](#)
- ["Installing CTE with No Key Manager Registration" on page 14](#)

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 more information about the available registration methods, see ["CTE Registration Method Options" on page 16](#).

For other installation options, see ["Installing CTE and Registering Using the Certificate Fingerprint Method" on page 22](#) and ["Installing CTE with No Key Manager Registration" on page 14](#).

Prerequisites

Note

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

Procedure

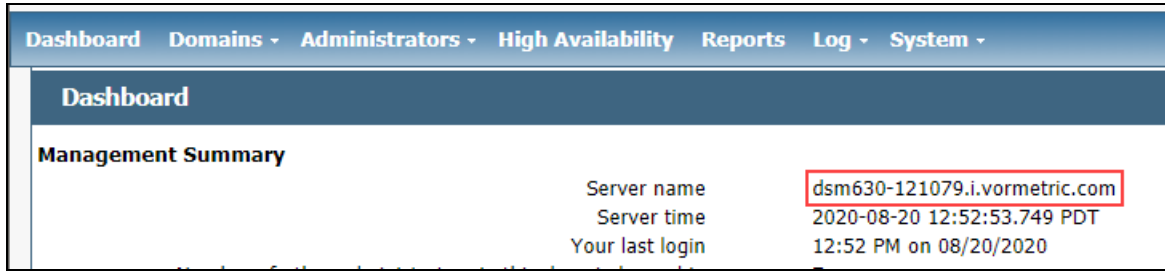
1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation file onto the Windows system.
3. Double-click the installation file. The InstallShield Wizard for CipherTrust Transparent Encryption opens.
4. Verify the version of CTE you are installing and click **Next**.
5. On the *License Agreement* page, accept the License Agreement and click **Next**.
6. On the *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.

7. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
8. 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.
9. In the Register Host dialog box, verify the host's machine name and click **Next**.
10. On the *Gathering agent information* page, select the **File System** check box and click **Next**.

11. 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.

12. 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 (see ["Host Name Resolution Requirements"](#) on page 17).
 - To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association \(Cloning Prevention\) Option"](#) on page 18.
 - 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-IDT feature available on the host, select the **Enable ES Feature** check box. For details about CTE-IDT, 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.

13. 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**.

14. Restart the host to complete the installation process.
15. 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 available registration methods, see ["CTE Registration Method Options" on page 16](#).

For other installation options, see ["Installing CTE and Registering Using the Shared Secret Registration Method" on page 20](#) and ["Installing CTE with No Key Manager Registration" on page 14](#).

Prerequisites

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

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

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

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

Note

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

Procedure

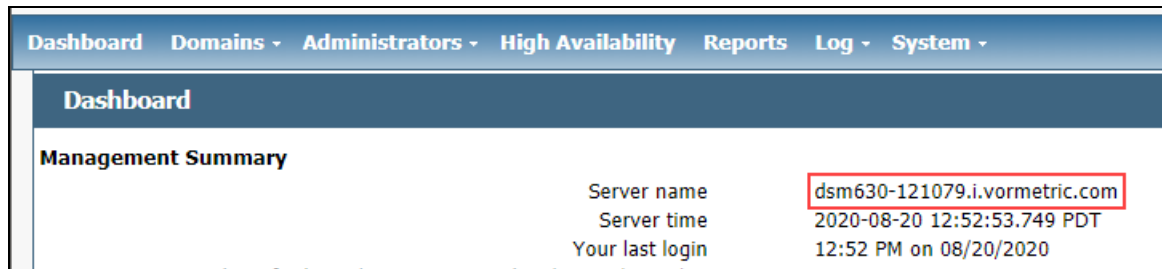
On the *InstallShield Wizard Completed* page, make sure the **Register CipherTrust Transparent Encryption now** check box is selected and click **Finish**. The installer opens the Register Host wizard.

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.



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.

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 (see ["Host Name Resolution Requirements" on page 17](#)).



WARNING

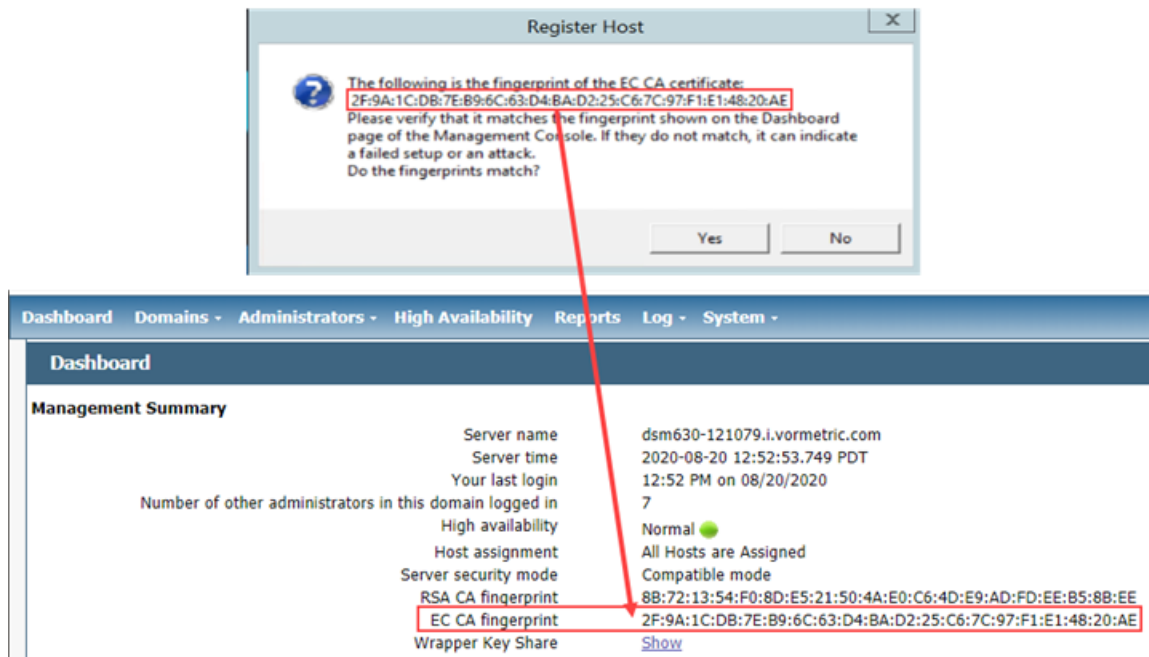
The host name specified here must exactly match the host name specified in the DSM in order for the fingerprints to match.

- To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association \(Cloning Prevention\) Option" on page 18](#).
- 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-IDT feature available on the host, select the **Enable ES Feature** check box. For details about CTE-IDT, 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 fingerprinting 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.

Silent Installation on Windows

Silent install refers to using the command line to install CTE in a non-interactive session. Use silent install to roll out CTE installations or upgrades to large numbers of hosts or to reduce your time and interaction as an administrator. Thales provides two types of installation binaries for silent installation:

- Self-extracting .exe
- Windows Installer Package (MSI).

Note: Thales supports installing or upgrading CTE agents with Microsoft System Center Configuration Manager (SCCM) using MSI installation binaries. For details, see your SCCM documentation.

For details, see one of the following procedures:

- ["Silent Installation Using the exe File and Shared Secret Registration Method" below](#)
- ["Silent Installation Using the MSI File and Shared Secret Registration Method" on page 28](#)
- ["Silent Installation Using the exe File and Fingerprint Registration Method" on page 31](#)
- ["Silent Installation Using the MSI File and Fingerprint Registration Method" on page 34](#)

For a combined list of all available silent install options for both the exe file and the MSI file, see ["All Windows Silent Install Command Line Options" on page 37](#).

Silent Installation Using the exe File and Shared Secret Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the exe file and the shared secret registration method. For a list of other available methods, see ["Silent Installation on Windows" on the previous page](#).

Prerequisites

Note

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

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `exe` file onto the Windows system.
3. Run the installation file using the following syntax:

```
<Installation_executable> /s /v" [ENABLE_LDT_CIFS=Yes] /qn INSTALLDIR=\"install-dir\" REGISTERHOSTOPTS=\"Options\"
```

where:

- If on a DSM, **ENABLE_LDT_CIFS=NO**.

Note: LDT for CIFS/NFS is not supported with DSM.

- `/s` (required) specifies that this is a silent install.
- `/v` (required) specifies that you want to pass command line options and values of public properties through to the installer.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTOPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

DSM host name

Required if you want to register CTE with a DSM.

-secret=shared-secret

Specifies the shared secret for the DSM.

This value is required for a DSM shared secret registration.

-domain=domain_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the domain name with which this CTE Agent will be associated.

-hostgroup=host/client_group_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the optional host/client group with which this host/client will be associated.

-agent=your.agent.name.com

FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

-useip

Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.

-description="description"

Specifies a description for the host. This description is displayed in the DSM.

If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.

-port=port

Specifies the port number this CTE Agent should use.

-usehwsig

Specify this option when you want to associate this installation with the machine hardware for cloning prevention.

-enableldt

Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.

-enablees

Specify this option automatically enable and register CTE-IDT for this host on your key manager during the silent install.

ENABLE_DOCKER

Set this value to 1 if you want to enable docker security on this host.

-log=%temp%\vor-agent-reg.log

Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).

-onewaycomms

Specify this option when CTE-initiated-only communication is required.

Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

to enable Cloud Object Storage during the silent install.

CERT_FIELD_PARAM

If you are using CTE-Cloud Object Storage, this option specifies a custom certificate field values for the CTE COS Root CA Certificate.

Note: If you want to enter an option with spaces in any value, it must be surrounded in two double-quotes with an escape character (\) before each double-quote. If the syntax is incorrect, the installation will fail.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- The CTE Agent will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be double-quoted, with each quote preceded by the escape character (\). For example: `INSTALLDIR="\\"C:\cte\custom dir\\""`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Again, the spaces in the description require the same syntax as in the installation directory name. For example: `-description="\\"This host was silently installed\\""`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> vee-fs-7.5.0-78-win64.exe /s /v" /qn
INSTALLDIR="\\"C:\cte\custom dir\\" registerhostopts="\my-key-mgr.example.com
-agent=my-host.example.com -secret=MaCarena45# -domain=my-domain -description="\\"This
host was silently installed\\""
```

Example: CTE-LDT, CTE-IDT, One-way Communication, Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-IDT (`-enablees` parameter), one-way communication

(`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.

- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).

```
C:\> vee-fs-7.5.0-78-win64.exe /s /v" /qn
registerhostopts=\"my-key-mgr.example.com -useip -enableldt -enablees
-onewaycomms -usehwsig -secret=MaCarena45# -domain=my-domain\""
```

Silent Installation Using the MSI File and Shared Secret Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the MSI file and the shared secret registration method. For a list of other available methods, see ["Silent Installation on Windows" on page 24](#).

Prerequisites

Note

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

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation MSI file onto the Windows system.
3. Run the installation file using the following syntax:

```
msiexe.exe /i <Installation_executable> [ENABLE_LDT_CIFS=Yes] /qn
INSTALLDIR=\"install-dir\" REGISTERHOSTOPTS=\"REGISTERHOSTOPTS_Options\"
```

where:

- If on a DSM, `ENABLE_LDT_CIFS=NO`.

Note: LDT for CIFS/NFS is not supported with DSM.

- `/i` (required) enables CTE installation.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTOPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

DSM host name

Required if you want to register CTE with a DSM.

-secret=shared-secret

Specifies the shared secret for the DSM.

This value is required for a DSM shared secret registration.

-domain=domain_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the domain name with which this CTE Agent will be associated.

-hostgroup=host/client_group_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the optional host/client group with which this host/client will be associated.

-agent=your.agent.name.com

FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

-useip

Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.

-description="description"

Specifies a description for the host. This description is displayed in the DSM.

If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.

-port=port

Specifies the port number this CTE Agent should use.

-usehwsig

Specify this option when you want to associate this installation with the machine hardware for cloning prevention.

-enableldt

Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.

-enablees

Specify this option automatically enable and register CTE-IDT for this host on your key manager during the silent install.

ENABLE_DOCKER

Set this value to 1 if you want to enable docker security on this host.

-log=%temp%\vor-agent-reg.log

Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).

-onewaycomms

Specify this option when CTE-initiated-only communication is required.

Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

to enable Cloud Object Storage during the silent install.

CERT_FIELD_PARAM

If you are using CTE-Cloud Object Storage, this option specifies a custom certificate field values for the CTE COS Root CA Certificate.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- The CTE Agent will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be in double-quotes. For example: `INSTALLDIR="C:\cte\custom dir"`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Because `-description` is inside a double-quoted string, you must escape the double-quotes `-description=\"This host was silently installed\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> msiexec.exe /i vee-fs-7.5.0-78-win64.exe /qn
INSTALLDIR="C:\cte\custom dir" registerhostopts="my-key-mgr.example.com
-agent=my-host.example.com -secret=MaCarena45# -domain=my-domain -description=\"This
host was silently installed\""
```

Example: CTE-LDT, CTE-IDT, One-way Communication, Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-IDT (`-enablees` parameter), one-way communication (`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).

```
C:\> msiexec.exe /i vee-fs-7.5.0-78-win64.exe /qn
registerhostopts="my-key-mgr.example.com -useip -enableldt -enablees -onewaycomms
-usehwsig -secret=MaCarena45# -domain=my-domain"
```

Example: CTE-LDT for CIFS Shares

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The CM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).

- This host will contain CIFS share GuardPoints (`ENABLE_LDT_CIFS=Yes`) and the CTE-LDT feature is enabled on the DSM (`-enableldt` parameter).
- The shared secret is `MaCarena45#` (`-secret` parameter) and the associated domain is `my-domain` (`-domain` parameter).

```
C:\> msixexec.exe /i vee-fs-7.5.0-78-win64.exe ENABLE_LDT_CIFS=Yes
/qn registerhostopts="my-key-mgr.example.com -useip -enableldt -secret=MaCarena45#
-domain=my-domain"
```

Note

CTE-LDT for NFS/CIFS feature is not supported with DSM. It is only supported with CipherTrust Manager.

Silent Installation Using the exe File and Fingerprint Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the exe file and the fingerprint registration method. For a list of other available methods, see ["Silent Installation on Windows" on page 24](#).

Prerequisites

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

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

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

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

Note

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

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `exe` file onto the Windows system.
3. Run the installation file using the following syntax:

```
<Installation_executable> /s /v" [ENABLE_LDT_CIFS=Yes] /qn INSTALLDIR=\"install-
dir\" REGISTERHOSTOPTS=\"Options\"
```

where:

- If on a DSM, `ENABLE_LDT_CIFS=NO`.

Note: LDT for CIFS/NFS is not supported with DSM.

- `/s` (required) specifies that this is a silent install.
- `/v` (required) specifies that you want to pass command line options and values of public properties through to the installer.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.

- `INSTALLDIR="install-dir"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHOSTOPTS="Options"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

DSM host name

Required if you want to register CTE with a DSM.

-domain=domain_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the domain name with which this CTE Agent will be associated.

-hostgroup=host/client_group_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the optional host/client group with which this host/client will be associated.

-agent=your.agent.name.com

FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

-useip

Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.

-description="description"

Specifies a description for the host. This description is displayed in the DSM.

If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.

-port=port

Specifies the port number this CTE Agent should use.

-usehwsig

Specify this option when you want to associate this installation with the machine hardware for cloning prevention.

-enableldt

Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.

-enablees

Specify this option automatically enable and register CTE-IDT for this host on your key manager during the silent install.

ENABLE_DOCKER

Set this value to 1 if you want to enable docker security on this host.

-log=%temp%\vor-agent-reg.log

Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).

-onewaycomms

Specify this option when CTE-initiated-only communication is required.

Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

to enable Cloud Object Storage during the silent install.

CERT_FIELD_PARAM

If you are using CTE-Cloud Object Storage, this option specifies a custom certificate field values for the CTE COS Root CA Certificate.

Note: If you want to enter an option with spaces in any value, it must be surrounded in two double-quotes with an escape character (\) before each double-quote. If the syntax is incorrect, the installation will fail.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- The CTE Agent will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be double-quoted, with each quote preceded by the escape character (\). For example: `INSTALLDIR=\\\"C:\cte\custom dir\\\"`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Again, the spaces in the description require the same syntax as in the installation directory name. For example: `-description=\\\"This host was silently installed\\\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> vee-fs-7.5.0-78-win64.exe /s /v" /qn  
INSTALLDIR=\\\"C:\cte\custom dir\\\" registerhostopts=\\\"my-key-mgr.example.com  
-agent=my-host.example.com -description=\\\"This host was silently installed\\\""
```

Example: CTE-LDT, CTE-IDT, One-way Communication, Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-IDT (`-enableids` parameter), one-way communication (`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.

```
C:\> vee-fs-7.5.0-78-win64.exe /s /v" /qn
registerhostopts=\"my-key-mgr.example.com -useip -enableldt -enablees
-onewaycomms -usehwsig\""
```

Example: CTE-LDT for CIFS Shares

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The CM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- This host will contain CIFS share GuardPoints (`ENABLE_LDT_CIFS=Yes`) and the CTE-LDT feature is enabled on the DSM (`-enableldt` parameter).

```
C:\>vee-fs-7.5.0-78-win64.exe /s /v" ENABLE_LDT_CIFS=Yes
/qn registerhostopts="my-key-mgr.example.com -useip -enableldt -domain=my-domain"
```

Note

CTE-LDT for NFS/CIFS feature is not supported with the DSM. It is only available on CipherTrust Manager.

Silent Installation Using the MSI File and Fingerprint Registration Method

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a DSM using the MSI file and the fingerprint registration method. For a list of other available methods, see ["Silent Installation on Windows" on page 24](#).

Note

Thales supports installing or upgrading CTE agents with Microsoft System Center Configuration Manager (SCCM) using MSI installation binaries. For details on how to do that, see your SCCM documentation.

Prerequisites

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

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

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

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

Note

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

Procedure

1. Log on to the host as a Windows user with System Administrator privileges.
2. Copy the CTE installation `MSI` file onto the Windows system.
3. Run the installation file using the following syntax:

```
msiexec.exe /i <Installation_executable> [ENABLE_LDT_CIFS=Yes] /qn  
INSTALLDIR=\"install-dir\" REGISTERHSTOPTS=\"REGISTERHSTOPTS_Options\"
```

where:

- If on a DSM, `ENABLE_LDT_CIFS=NO`.

Note: LDT for CIFS/NFS is not supported with DSM.

- `/i` (required) enables CTE installation.
- `/qn` (required) specifies that the install should be non-interactive and that no GUI should be displayed.
- `INSTALLDIR=\"install-dir\"` is an optional parameter specifying the installation directory you want to use. If you omit this parameter, CTE installs in the directory `C:\Program Files\Vormetric\DataSecurityExpert\agent\`

Note: Thales recommends that you install CTE in the default directory if at all possible.

- `REGISTERHSTOPTS=\"Options\"` (required if you want to register CTE) is a list of options that you want the installer to use. The common options are:

DSM host name

Required if you want to register CTE with a DSM.

-domain=domain_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the domain name with which this CTE Agent will be associated.

-hostgroup=host/client_group_name

Note: For Shared Secret only (not DSM Fingerprint)

Specifies the optional host/client group with which this host/client will be associated.

-agent=your.agent.name.com

FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

-useip

Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.

-description="description"

Specifies a description for the host. This description is displayed in the DSM.

If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.

-port=port

Specifies the port number this CTE Agent should use.

-usehwsig

Specify this option when you want to associate this installation with the machine hardware for cloning prevention.

-enableldt

Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.

-enablees

Specify this option automatically enable and register CTE-IDT for this host on your key manager during the silent install.

ENABLE_DOCKER

Set this value to 1 if you want to enable docker security on this host.

-log=%temp%\vor-agent-reg.log

Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).

-onewaycomms

Specify this option when CTE-initiated-only communication is required.

Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

to enable Cloud Object Storage during the silent install.

CERT_FIELD_PARAM

If you are using CTE-Cloud Object Storage, this option specifies a custom certificate field values for the CTE COS Root CA Certificate.

Example: Custom Install Directory and Host Description with Spaces

The following example specifies that:

- The CTE Agent will be installed in the custom directory `C:\cte\custom dir`. The spaces in the installation directory name require it to be in double-quotes. For example: `INSTALLDIR="C:\cte\custom dir"`.
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using the host name `my-host.example.com` (`-agent` parameter).
- The host will be registered with the description `This host was silently installed` (`-description` parameter). Because `-description` is inside a double-quoted string, you must escape the double-quotes `-description=\"This host was silently installed\"`

Note

The examples below are shown on several lines for readability. When you enter the command, all parameters should be on the same line.

```
C:\> msiexec.exe /i vee-fs-7.5.0-78-win64.exe /qn  
INSTALLDIR="C:\cte\custom dir" registerhostopts="my-key-mgr.example.com  
-agent=my-host.example.com -description=\"This host was silently installed\""
```

Example: CTE-LDT, CTE-IDT, One-way Communication, Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The DSM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- The CTE-LDT (`-enableldt` parameter), CTE-IDT (`-enablees` parameter), one-way communication (`-onewaycomms` parameter) and hardware association (`-usehwsig` parameter) features are enabled.

```
C:\> msixexec.exe /i vee-fs-7.5.0-78-win64.exe /qn  
registerhostopts="my-key-mgr.example.com -useip -enableldt -enablees -onewaycomms  
-usehwsig"
```

Example: CTE-LDT for CIFS Shares

Note

CTE-LDT for NFS/CIFS is not supported with DSM. It is only supported with CipherTrust Manager.

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the `INSTALLDIR` parameter is omitted).
- The CM host name is `my-key-mgr.example.com`.
- The host will be registered using its IP address and not its host name (`-useip` parameter).
- This host will contain CIFS share GuardPoints (`ENABLE_LDT_CIFS=Yes`) and the CTE-LDT feature is enabled on the DSM (`-enableldt` parameter).

```
C:\> msixexec.exe /i vee-fs-7.5.0-78-win64.exe ENABLE_LDT_CIFS=Yes  
/qn registerhostopts="my-key-mgr.example.com -useip -enableldt -domain=my-domain"
```

All Windows Silent Install Command Line Options

The MSI and self-extracting `.exe` silent install methods require different command line options to specify a silent installation. However, the parameters specific to CTE installation are the same for both MSI and self-extracting `.exe` install methods. See the following tables for required and optional command line options.

For a specific silent install procedure, see one the following:

- ["Silent Installation Using the exe File and Shared Secret Registration Method" on page 25](#)
- ["Silent Installation Using the MSI File and Shared Secret Registration Method" on page 28](#)
- ["Silent Installation Using the exe File and Fingerprint Registration Method" on page 31](#)
- ["Silent Installation Using the MSI File and Fingerprint Registration Method" on page 34](#)

General Format for Self-extracting .exe Silent Install Commands

For self-extracting `.exe` silent installations, be sure to escape the quotes surrounding the parameters passed in `REGISTERHOSTOPTS_Options` using a backslash (`\`) as shown:

```
<Installation_executable> /s /v" [ENABLE_LDT_CIFS=Yes] /qn  
REGISTERHOSTOPTS=\"REGISTERHOSTOPTS_Options\"
```

For example:

```
vee-fs-7.5.0-78-win64.exe /s /v" ENABLE_LDT_CIFS=Yes /qn  
REGISTERHSTOPTS=\"SecSrv.demo.com -useip\""
```

General Format for MSI Silent Install Commands

Use the following syntax for MSI silent installations:

```
msiexe.exe /i <Installation_executable> [ENABLE_LDT_CIFS=Yes] /qn  
REGISTERHSTOPTS="REGISTERHSTOPTS_Options"
```

For example:

```
msiexec.exe /i vee-fs-7.5.0-78-win64.msi ENABLE_LDT_CIFS=Yes /qn REGISTERHSTOPTS="  
SecSrv.demo.com -useip"
```

Command Line Options for MSI and .exe Silent Installations

Refer to the following tables for required and optional command line options for MSI and self-extracting .exe CTE silent installations.

The following table lists the command line options for self-extracting .exe binary types.

Windows Attribute	Description	Required?
/s	Run the installation in silent mode.	Yes
/v	Pass command-line options and values of public properties through to the installer.	Yes

The following table lists the command line options for MSI binary types.

Windows Attribute	Description	Required?
/i	Enable installation/configuration	Yes, for installation
REINSTALLMODE=voums	Required REINSTALLMODE codes for upgrades	Yes, for upgrade
REINSTALL=ALL	Required REINSTALL setting for upgrades	Yes, for upgrade
/x	Required for uninstallation. See Chapter 13: "Uninstalling CTE from Windows" on page 123.	Yes, for uninstall

The following table lists the command line options common to both MSI and self-extracting .exe binary types.

Windows Attribute	Description	Required?
ENABLE_LDT_CIFS=Yes Note: CTE-LDT for NFS/CIFS is not supported with DSM. It is only supported on CipherTrust Manager.	ENABLE_LDT_CIFS=Yes is an optional parameter that indicates you plan to use CTE-LDT with CIFS share GuardPoints on this host with CM. If you specify this option, you will <i>not</i> be able to guard any local directories on this host, even if those directories use a Standard CTE policy. Only CTE-LDTGuardPoints on CIFS shares will be supported for this host. If you plan to create local file system GuardPoints on this host, omit this parameter or specify ENABLE_LDT_CIFS=No. If you do this, you will <i>not</i> be able to use CTE-LDT with any CIFS share GuardPoints on this host. Note: If you are specifying this option, make sure you also include <code>-enableldt</code> in the REGISTERHOSTOPTS parameter in order to enable CTE-LDT for this host in the DSM.	
/qn	Run the command in non-interactive mode (no GUI).	Yes
REGISTERHOSTOPTS	Options for registering CTE with the DSM. The full set of options is specified below.	No
INSTALLDIR	Specifies an alternate location for installing CTE. Notes: <ul style="list-style-type: none"> • If syntax is incorrect, silent install will fail. See examples. • The alternate location must be on the system drive. 	No
REBOOT=ReallySuppress	By default, the machine reboots after installation. Supplying this option prevents that. However, a reboot is still required to fully install CTE.	No

The following table lists the REGISTERHOSTOPTS parameters that determine log settings and CTE configuration settings. The REGISTERHOSTOPTS parameters are common to both MSI and self-extracting .exe binary types.

DSM host name

Required if you want to register CTE with a DSM.

-secret=shared-secret

Specifies the shared secret for the DSM.

This value is required for a DSM shared secret registration.

-domain=domain_name

Note

For Shared Secret only (not DSM Fingerprint)

Specifies the domain name with which this CTE Agent will be associated.

-hostgroup=host/client_group_name

Note

For Shared Secret only (not DSM Fingerprint)

Specifies the optional host/client group with which this host/client will be associated.

-agent=your.agent.name.com

FQDN of the host on which the CTE Agent is being installed. If this value is not specified, the installer uses the host's IP address.

-useip

Use the IP address of the protected host instead of host name. Used when `-agent` is not supplied.

-description="description"

Specifies a description for the host. This description is displayed in the DSM.

If an entry for this host already exists in the DSM and the host already has a description, CTE does *not* overwrite the existing description even if this option is specified.

-port=port

Specifies the port number this CTE Agent should use.

-usehwsig

Specify this option when you want to associate this installation with the machine hardware for cloning prevention.

-enableldt

Specify this option to automatically enable and register CTE-LDT (Live Data Transformation) for this host on your key manager during the silent install.

-enableees

Specify this option automatically enable and register CTE-IDT for this host on your key manager during the silent install.

ENABLE_DOCKER

Set this value to 1 if you want to enable docker security on this host.

-log=%temp%\vor-agent-reg.log

Specifies a log file particular to the registration. Useful for documenting why the registration failed (if it does).

-onewaycomms

Specify this option when CTE-initiated-only communication is required.

Thales recommends that you use two-way communication between CTE and the key manager whenever possible.

to enable Cloud Object Storage during the silent install.

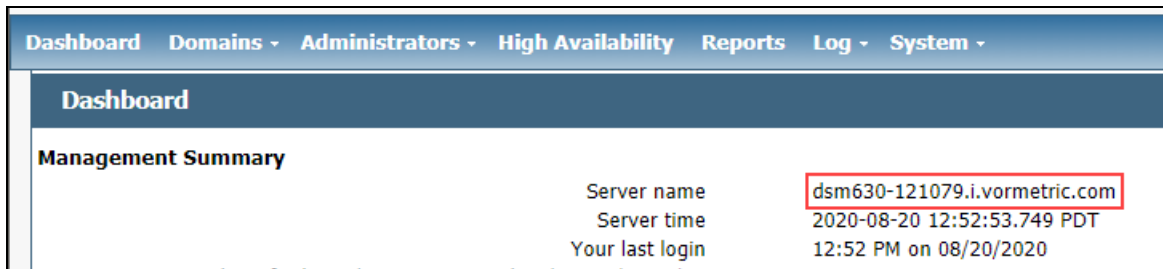
CERT_FIELD_PARAM

If you are using CTE-Cloud Object Storage, this option specifies a custom certificate field values for the CTE COS Root CA Certificate.

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

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see "[Installing CTE and Registering Using the Certificate Fingerprint Method](#)" on page 22 or "[Installing CTE and Registering Using the Shared Secret Registration Method](#)" on page 20.

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe`.
3. In the Register Host dialog box, verify the host's machine name and click **Next**.
4. On the *Gathering agent information* page, select the **File System** check box and click **Next**.
5. 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.

6. 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 (see ["Host Name Resolution Requirements" on page 17](#)).
 - To enable cloning prevention, select the **Enable Hardware Association** check box. For details, see ["Hardware Association \(Cloning Prevention\) Option" on page 18](#).
 - 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-IDT feature available on the host, select the **Enable ES Feature** check box. For details about CTE-IDT, 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.

7. 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**.

8. Restart the host to complete the installation process.
9. 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.

Registering CTE with the Fingerprint Registration Method After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete. If you have not yet installed the CTE Agent, see "[Installing CTE and Registering Using the Certificate Fingerprint Method](#)" on page 22 or "[Installing CTE and Registering Using the Shared Secret Registration Method](#)" on page 20.

Prerequisites

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

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

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

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

Note

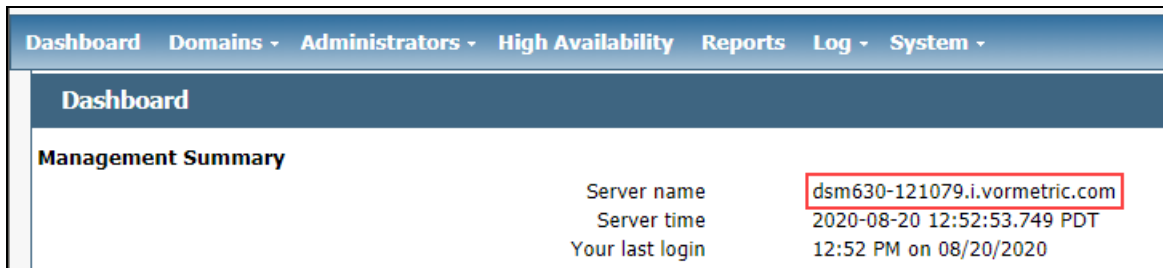
If registration appears to freeze, verify that the DSM and CTE can communicate with each other over the network.

Procedure

1. Log on to the host as a Windows user with administrative privileges.
2. Launch the CTE Registration Wizard using one of the following methods:
 - In the system tray, right click the CipherTrust Lock icon and select **Register Host**.
 - Run `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe`.
3. 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.

4. On the *Gathering agent information* page, select the **File System** check box and click **Next**.
5. 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.

6. 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 (see "[Host Name Resolution Requirements](#)" on page 17).



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. For details, see "[Hardware Association \(Cloning Prevention\) Option](#)" on page 18.
- 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-IDT feature available on the host, select the **Enable ES Feature** check box. For details about CTE-IDT, 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.

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

The screenshot shows a 'Register Host' dialog box with the following text: "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?" Below the dialog box is a 'Management Summary' dashboard with the following data:

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**.

8. 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**.
9. Restart the host to complete the installation process.
10. 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.

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**.

The screenshot shows the 'Add Policy - Simple-Policy' page. At the top, there is a navigation bar with 'Policies' selected. The main form has the following fields:

- Policy Type:** Standard (dropdown)
- Name:** Simple-Policy (text input, highlighted with a red box)
- Description:** This is a simple, Standard Policy (text input)
- Learn Mode:** unchecked checkbox
- Clone this policy as:** empty text input with a 'Clone' button

Below the form are two tables:

- Security Rules:** A table with columns: Select, Order, Resource, User, Process, Action, Effect, When, Browsing. It shows 0 rows.
- Key Selection Rules:** A table with columns: Select, Order, Resource, Key. It has 1 row with 'Simple-Policy-Key' in the 'Key' column, which is highlighted in yellow and has a red box around it.

At the bottom right, there are 'Ok', 'Apply', and 'Cancel' buttons.

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\

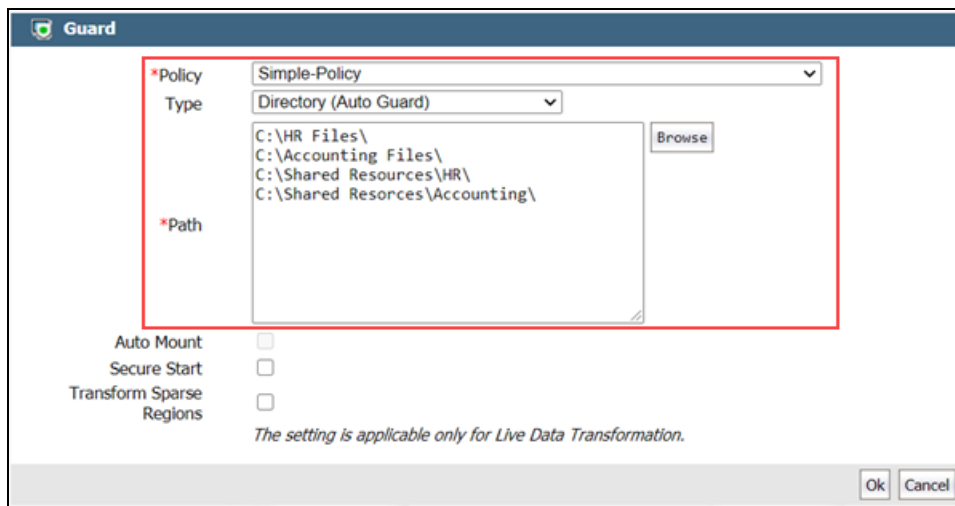
Note

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:



- 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.)

Chapter 3: Special Cases for CTE Policies

This chapter describes some CTE-specific configuration tasks related to configuring policies in the key manager. It contains the following topics:

More Information About Configuring CTE Policies	48
Re-Signing Executable Files on Secfs GuardPoints	48
Re-Enabling Automatic Signing for Host Settings	49
Behavior of Hard Links Inside and Outside of GuardPoints (Windows)	49

More Information About Configuring CTE Policies

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

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

Re-Signing Executable Files on Secfs GuardPoints

If any of your existing VTE for Windows hosts are running VTE versions prior to version 6.2.0, an issue affects signed executables in Live Data Transformation policies. In these older VTE versions, any executable that is part of either a host setting or a Signature set, and resides in a GuardPoint that uses a Live Data Transformation policy will have a different SHA signature after every LDT key rotation. After each LDT key rotation, the host settings executables will no longer be authenticated, or the Signature Set policy rules that include those executables will no longer match them as expected. This problem occurred because VTE generated an SHA signature of the encrypted executable which changes after each key rotation. To work around these issues on these older VTE versions, the DSM Security Administrator must manually re-sign each affected executable after each key rotation. This workaround is *not* needed for any VTE for Windows release version 6.2.0 or later.

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

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

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

Note

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

Re-Enabling Automatic Signing for Host Settings

CTE blocks automatic re-signing of the host settings. Some users may have established procedures for updating system software that are based on the assumption that restarting the `vmd` will generate new signatures when signed software is updated. This is no longer true. However, you can re-enable automatic re-signing if your environment requires it.



CAUTION

Re-enabling the automatic regeneration of signatures exposes a potential security vulnerability for CTE Agents. When enabled, host setting binaries are re-signed when CTE receives a push from the associated key manager. If an attacker were to replace a binary with a Trojan, and then force a push from the key manager by, for example, restarting the CTE Agent, CTE could generate a signature for the malicious binary and pass it.

To re-enable automatic re-signing for host settings:

1. Change to the directory where the `agent.conf` file resides. For example, type:

```
# cd /opt/vormetric/DataSecurityExpert/agent/vmd/etc/
```

2. Edit the `agent.conf` file.

3. Change or add the following line:

```
AUTO_RESIGN_HOST_SETTINGS=TRUE
```

4. Save your changes and exit the file.

5. Restart the `vmd` to set the changes. Type:

6. Type the following to verify that the host settings is set to true:

```
# vmsec vmdconfig
```

Behavior of Hard Links Inside and Outside of GuardPoints (Windows)

When using hard links on Windows, all the hard links to a file must be within the boundary of a GuardPoint and must use the same key. The following scenarios provide additional details:

- If hard links to the same file are inside a GuardPoint and outside a GuardPoint, the effect on the file depends on what process accesses which hard link first. If the hard link within the GuardPoint is opened first, the file is transformed. If the hard link outside the GuardPoint is opened first, the file won't be transformed.
- If hard links to the same file exist in different GuardPoints with different keys, the file will be corrupted.
- If hard links to the same file exist in the same GuardPoint but with different keys, such as if folder-based rules are used, there will be a conflict in the key.

Chapter 4: Enhanced Encryption Mode

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

- Compatibility 50
- Disk Space 51
- Encryption Migration 51
- File Systems Compatibility 51
- FileTable Support on Windows 52
- Using the AES-CBC-CS1 Encryption Mode in DSM 52
- Exceptions and Caveats 53
- Best Practices for AES-CBC CS1 Keys and Host Groups 53

The AES-CBC-CS1 encryption is superior to the existing AES-CBC mode because it uses a unique and unpredictable (random) IV (initialization vector) generated for each individual file. The per-file IV object is generated only at file creation time. It is stored as file metadata.

Note
AES-CBC-CS1 encryption does not require any additional license.

	AES-CBC	AES-CBC-CS1
Security Improvements		
Unique IV per-file	No	Yes
IV predictability	Yes	No
File System Support		
Local FS	NTFS/ReFS	NTFS/ReFS
Remote FS	CIFS	No support
Block Device Support (secvm)	Fully supported	No. When a policy contains a key with CBC-CS1 encryption mode, the guarding fails on the DSM, and an error message displays.

Compatibility

- Starting with VTE for Windows version 6.1.0, CTE is backward compatible with, and fully supports, the existing AES-CBC mode for both new and existing datasets.
- Starting with VTE for Windows version 6.1.0, CTE fully supports AES-CBC-CS1 encryption for LDT and offline data transformation on CTE Windows environments.
Versions of VTE prior to version 6.1.0 are *not* backwards compatible with AES-CBC-CS1 encryption. On these earlier versions, attempting to guard a device using a policy containing an AES-CBC-CS1 key will fail.
- Protected hosts supporting AES-CBC-CS1 encryption can be added to host groups.

Difference between AES-CBC and AES-CBC-CS1

The two encryption modes are completely different from a file format standpoint.

- AES-CBC-CS1 encryption only applies to file system directories; AES-CBC encryption applies to both files and block devices.

Notes

- If you attempt to use an AES-CBC-CS1 key to guard a block device or partition, the guarding fails with an error reported on the DSM, similar to: Raw or Block Device (Manual and Auto Guard) GuardPoints are incompatible with Policy “policy-xxx” that contains a key that uses the CBC-CS1 encryption mode.”
- While AES-CBC-CS1 encryption is supported on both Linux and Windows environments, the file formats are incompatible. An encrypted file created with a specific AES-CBC-CS1 key on Windows cannot be read on Linux, even if that specific key were to be used and vice versa.

- AES-CBC-CS1 uses cipher-text stealing to encrypt the last partial block of a file whose size is not aligned with 16 bytes.
- Each file encrypted with an AES-CBC-CS1 key is associated with a unique and random base IV.
- AES-CBC-CS1 implements a secure algorithm to tweak the IV used for each segment (512 bytes) of a file.

Disk Space

Files encrypted with AES-CBC-CS1 keys consume additional disk space in contrast to files encrypted with AES-CBC keys. This is because AES-CBC-CS1 encryption requires file IVs to be created and persistently stored in contrast to AES-CBC encryption which does not consume any additional disk storage.

Therefore, administrators need to plan and provision additional disk capacity prior to deploying AES-CBC-CS1 encryption.

	AES-CBC	AES-CBC-CS1
Local Windows FS	No change to file size. No ADS allocation.	Extra 4KB allocation (at minimum) in the form of an embedded header per file. With CTE guarding enabled, file size expansion is hidden.

Encryption Migration

You can use either LDT or offline dataxform to:

- Transform data encrypted by AES-CBC to AES-CBC-CS1 and vice versa.
- Transform AES-CBC-CS1 encrypted data to clear contents and vice versa.

File Systems Compatibility

On Windows, you can use AES-CBC-CS1 keys to guard currently supported file systems.

Note

The remote file system must have enough extra space to store the extra 4K bytes of the embedded header.

Storing Metadata

AES-CBC-CS1 encrypted files on Windows store the base IV of a file in a Windows ADS (Alternate Data Streams) associated with the file. The size required for saving the CS1 key depends on the allocation size of the file system. If the allocation size is set to 4k, then the new IV will require 4K of extra space on the disk. You can run the `fsutil`

`fsinfo` tool to find out the allocation size of the file system.

The CS1 key is supported on following file systems:

- **NTFS**: Supported on all Windows platforms that are supported by CTE.
- **REFS**: Supported on Windows 2012 R2 and later.
- **CIFS**: Supported if the backend storage for the CIFS share is Windows-based storage.

Note

Some network storage servers do not support multiple ADS associated with a file.

To get the value of the base IV, type:

```
C:/>voradmin secfs iv get <file-name>
```

Note

The base IV of a file is protected. It cannot be set/modified/removed by commands and applications. However, if a GuardPoint is unguarded, the files in the GuardPoint are no longer protected. An adversary can then corrupt the content of the files, as well as the IVs.

AES-CBC-CS1 depends on the physical file system's support for extended attributes in a manner similar to the CipherTrust Transparent Encryption - Live Data Transformation feature.

Missing IV file

If the IV for a file is missing, or CTE is unable to read the IV, then CTE denies access to the file. This access denied message may trigger an application to display an error message. This message may vary from application to application.

	AES-CBC	AES-CBC-CS1
Local FS (Windows)	No change	Alternate Data Streams

FileTable Support on Windows

The CBC-CS1 key does not support FileTables. This is because FileTables do not support alternate data streams. The CS1 key requires the ability to write the per-file IV into an alternate data stream on each file.

Using the AES-CBC-CS1 Encryption Mode in DSM

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

1. In the DSM, click **Keys > Agent Keys > Keys**.
2. Click **Add**.
3. In the Encryption Mode dropdown, select **CBC-CS1**.
4. In the Algorithm dropdown, select **AES128** or **AES256** to create an AES-CBC-CS1 key.
5. Edit or create a policy that will use the AES-CBC-CS1 key. In this policy:
 - In the **Key Selection Rules** section, click **Add** and select the AES-CBC-CS1 key.
6. Click **OK** to save the policy.
7. Push the policy to the GuardPoints that you want to use this encryption key.

Exceptions and Caveats

Note the following when using AES-CBC-CS1 keys.

Guarding Existing Files Without Data Transformation

You must convert an existing file with clear text through offline data transformation or LDT. If you do not transform the file, then after you guard using an AES-CBC key, the file displays garbled characters.

If you use an AES-CBC-CS1 key, access to the file is blocked with an I/O error.

Best Practices for AES-CBC CS1 Keys and Host Groups

In a host group, do not deploy policies associated with AES-CBC and AES-CBC CS1 keys unless all hosts are running VTE for Windows version 6.1.0 or CTE version 7.0.0 or later.

Chapter 5: Utilities for CTE Management

Thales provides a variety of utilities that augment the standard Windows utilities. This combination of tools helps administrators manage CTE. The following utilities are described in this chapter:

voradmin secfs Commands	54
vmsec Utility	56
agenthealth Utility	57
agentinfo Utility	58
Backup Utility	59

voradmin secfs Commands

The `voradmin secfs list` and `voradmin secfs status` commands display GuardPoint and policy information on the host.

voradmin secfs List Commands

The `voradmin secfs list` command has the following options:

voradmin secfs list Options

<code>guardpoints</code>	Displays all the GuardPoints on the host.
<code>policy</code>	Displays all the policies used on the host.
<code>logger</code>	Displays the logging details on the host.
<code>status</code>	Displays the authentication settings on the host.

For example, to view all the GuardPoints on the host, type:

```
C:\>voradmin secfs list guardpoints
Guard Point:      1
Policy ID:        16553
Policy name:      ES-Standard-Policy
Directory:        esg-disk1-demo
Type:             rawdevice
Status:           guarded

Guard Point:      2
Policy ID:        18857
Policy name:      Accounting-IT-Access-Policy
Directory:        G:\Data
Type:             local
Status:           guarded

Guard Point:      3
Policy ID:        18985
Policy name:      LDT-Policy
Directory:        C:\LDT-Folder
Type:             local
Status:           guarded
```

To view just the policies in use on the host, you would enter:

```
C:\>voradmin secfs list policy
Policy:           1
Policy name:      LDT-Policy
Type:             LDT

Policy:           2
Policy name:      ES-Standard-Policy
Type:             ONLINE

Policy:           3
Policy name:      Accounting-IT-Access-Policy
Type:             ONLINE
```

voradmin secfs status Commands

The `voradmin secfs status` command has the following options:

voradmin secfs status Options

keys	Displays the current status of the keys on the host.
lock	Displays the status of any system or agent locks on the host.
crypto	Displays the encryption modes that are supported.

For example:

```
C:\> voradmin secfs status keys

Encryption keys are available

C:\> voradmin secfs status lock

FS Agent Lock: Disabled
System Lock: Disabled

C:\> voradmin secfs status crypto

AES CBC, CBC_CS1, XTS modes are supported

Encryption key protection is supported
```

vmsec Utility

The `vmsec` utility allows you to manage the security aspect of the CTE Agent on the host. On Windows the `vmsec` utility is `<windows-agent-install-dir>\vmd\bin\vmsec.exe`. The default path is:

```
C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmsec.exe
```

vmsec Syntax

<code>check_install</code>	Verifies that the kernel component is running. This command checks CTE services and reports if any of the services are not running.
<code>challenge</code>	Initiates challenge-response on the host. This command displays a CTE Agent password challenge string and enter the response string when the key manager is not network accessible.
<code>status</code>	Displays kernel configuration.
<code>vmdconfig</code>	Displays the vmd configuration.
<code>check_hwenc</code>	Determines whether this system supports hardware crypto.
<code>hwok</code>	Reports status of hardware signature.
<code>passwd [-p passwd]</code>	Enters the host password when the key manager is not network accessible. User can unlock the GuardPoints with this password.
<code>version</code>	Displays the CTE version.

Displaying the CTE Challenge String

In addition to using `vmsec challenge` on Windows, you can also right-click the tray icon and select **Challenge...-> Response**. The *CTE Challenge/Response* window opens.

If no challenge string is displayed, the host password is static. If a challenge string displays, contact a Administrator for the response string.

Using the CTE Challenge String

When communication with the DSM is unavailable, the agent pauses on access to guarded directories. The agent waits for communication to be restored or a challenge/response to be issued and completed. The agent notifies the user of this condition and requests the challenge/response with log messages in `dmesg` and `vmd.log` in five minute intervals.

agenthealth Utility

The `agenthealth.ps` utility validates:

- Super-user privilege
- CTE Agent installation
- CTE registration to key manager
- CTE processes/modules that are running
- Available disk resources:
- Current GuardPoints: Tests if the agent can reach the GuardPoints
- CTE log directory resource status

This directory contains pending CTE log files for upload. This utility reports the size and number of pending files for upload. These text files are logs that contain `vmd/SecFS` information. They are regenerated whenever `secfs` restarts. If the number of files is unexpectedly large, this can indicate a problem.

Agent Health Check Script

The Agent health check script (`agenthealth.ps1`) is located in `C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\`

To run the `Agenthealth` check script:

1. Run the power shell command to enable self-signing for the system.
Before running `agent-health` script make sure power shell command has enough privileges to execute the Powershell script. Some Windows operating systems have default execution policy set as `restricted`.
Use the Powershell command `Set- Execution-policy Remote Signed` to change the execution policy if needed.
2. Open the Powershell prompt as administrator.
3. Type:
`.\agenthealth.ps1`

System Response

```
Log file is at log\agent_health.log
Checking super user privilege..... OK
Vormetric Agent installation..... OK
Vormetric policy directory..... OK
Registration to server..... OK
Kernel drivers are loaded..... OK
VMD is running..... OK
SECFS is running..... OK
```

```
rhat26130.qa1.com is resolvable.....K.....OK
rhat26130.qa1.com port 8446 is reachable..... OK
rhat26130.qa1.com port 8447 is reachable..... OK
Can communicate to at least one server..... OK
VMD is listening on port 7024..... OK
Time of last update from server    2016-12-01    14:39:49.038
Checking available disk space..... OK
Checking logging space ..... OK
    Log directory is ""
    File system for log data is "/", 32G free (17% full)
    Log directory contains 2 of maximum 200 files (1% full)
    Log directory contains 1 of maximum 100 Mbytes used (1% full)
Testing access to C:\GP2..... OK
```

agentinfo Utility

The `agentinfo` utility collects system logs, CTE agent logs, CTE agent trace information, and system information for diagnostic purposes. All this information is saved in the destination path and compressed into a zip file. The `agentinfo` utility is available as an `agentinfo.js` Java command and as an `agentinfo.ps1` PowerShell command.

agentinfo Utility (Java version)

The `agentinfo.js` utility is a JavaScript file. You can open it in a text editor to see specific functions.

The `agentinfo.js` support collection scripts reside in the following path on systems where the CTE agent is installed.

To run the `agentinfo` script on Windows, navigate to one of the following folders:

```
C:\Program
Files\Vormetric\DataSecurityExpert\agent\vmd\bin
```

or

```
C:\Program
Files\Vormetric\DataSecurityExpert\agent\shared\bin
```

then run the following script:

```
agentinfo.js
```

agentinfo Utility (PowerShell version)

The PowerShell version of `agentinfo` supports several parameters.

PowerShell version agentinfo parameters

Directory - Specify the directory where all the collection information is saved. By default, this information is saved in the current directory.

ZipFile - Specify the name of the compressed file, where all the collected information will be archived. By default, this information is saved in the current directory.

Logfile - Specify the name of the files where verbose logs will be saved. By default, this information is saved in the current directory.

Examples for using agentinfo utility (PowerShell version)

To save all the collection information in “c:\AgentLogs” folder, run the following command:

```
.\agentinfo.ps1 -Directory 'C:\AgentLogs'
```

To save all the collected information in “c:\AgentLogs” folder and verbose logs in “c:\temp\AgentInfo.log”, run the following command:

```
.\agentinfo.ps1 -Directory 'C:\AgentLogs' -LogFile 'c:\temp\AgentInfo.log'
```

To save all the collected information in “c:\AgentLogs” folder, verbose logs in “c:\temp\AgentInfo.log”, and create the “AgentInfo.zip” archive file, run the following command:

```
.\agentinfo.ps1 -Directory 'c:\AgentLogs' -LogFile 'c:\temp\AgentInfo.log' -ZipFile 'C:\temp\AgentInfo.zip'
```

Note

PowerShell 5.1 or later is required. Use the `$PSVersionTable.PSVersion` command to confirm which PowerShell version you are using.

Backup Utility

When a backup is performed, certain files and directories may be protected against access. Therefore, those files and directories are not written to the backup repository. These include files located in the Data Transformation GuardPoints or files in GuardPoints with appropriate policies. Additionally, the following files are locked by default by CTE agent:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The following describes how to bypass the issue for multiple scenarios:

Agent is installed in the default location

1. Stop SecFS, type: `/etc/vormetric/ stop`
2. Run the backup application with the desired arguments.
3. Restart SecFS, type: `/etc/vormetric/ start`

Using a backup image to install to other agents or restore to a different system

When the image is used to reinstall the system, the agent will automatically start at system boot and will attempt to connect to the key manager to which it was originally registered.

To prevent multiple systems with the same agent ID, you must uninstall CTE from the system before running the backup application. The restore/install from the backup will not have an agent running.

1. Uninstall the agent, type `/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsfs`
2. Run the backup application with the desired arguments.
3. Re-install CTE agent.

Performing a backup while the agent is running

Before running the backup application, add the files that are protected by the agent to the exclusion rules to exclude them from the backup:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/.access  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/etc/*  
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec/pem/*
```

The GuardPoint policy may implement access restrictions which would also cause the backup application to generate error messages. These GuardPoints/directories will also need to be added to the exclusion rule method to exclude them from the backup. Alternatively, you can temporarily unguard them while the backup application is running.

If the CTE agent reports a status of incomplete in the backup application and does not start properly, or partially starts but generates error messages at system boot time, then uninstall and reinstall the agent. The restore/clone image contains everything needed to uninstall the agent. Use the following command to perform this operation:

```
/opt/vormetric/DataSecurityExpert/agent/secfs/bin/uninstallsfs
```

Chapter 6: Using CTE with Microsoft SQL

This chapter discusses using CTE with Microsoft SQL AlwaysOn and SQL File Tables. It contains the following topics:

Using CTE with SQL	61
Using LDT with SQL FILESTREAM	61
Using CTE with SQL FileTables	61
Installing CTE on Microsoft SQL AlwaysOn	63
Data Transformation (Encryption in place)	67
Copy/Restore	67
SQL Server Policy Tuning	67
Using LDT with SQL AlwaysOn	67

Using CTE with SQL

You must stop the SQL service before guarding the SQL DB. When this occurs, the SQL Server replication may become unsynchronized. When restarting, it may take a brief period of time for the SQL Server replication to resynchronize with the other node. The SQL Server issues a warning against any attempted failovers during that brief period.

Note

Minimizing the duration for which the SQL Server service is stopped is beneficial for reducing the resynchronization period.

Using LDT with SQL FILESTREAM

When applying a Live Data Transformation (LDT) GuardPoint to SQL Server with FILESTREAM enabled, a rekey may be triggered which never finishes. This can occur if SQL Server is renaming files when the GuardPoint is applied, which causes the rekey to start the scan process again. If the rekey seems to be taking a long time, stop the SQL service until the rekey finishes and then restart the SQL service.

Using CTE with SQL FileTables

SQL FileTables allows you to store files and documents in special tables in the SQL Server called FileTables, but access them from Windows applications as if they were stored in the file system, without making any changes to your client applications. For some of the use cases, you can use FileTables with CTE.

Considerations

- The CTE Agent must be installed on the same server where the FileTables reside. If the FileTables reside on your SQL server, then you should install the CTE Agent on your SQL server.
- If multiple servers access the SQL FileTables:
 - Install CTE agent on all of the servers.
 - Protect all of the FileTable folders with the same CTE policy.



CAUTION

Accessing the FileTable without CTE may corrupt the data.

- When you create a new FileTable, alter, or drop FileTables, this may require applying a new GuardPoint.
- Every FileTable has a separate FileTable Folder so you must apply separate GuardPoints for each FileTable.
- You must apply a unique GuardPoint to each VNN path.
For example, if you configure two FileTables on an SQL Server, then the remote SQL administrator system must apply one GuardPoint to each configured VNN name.
- Guarding on a VNN name is similar to guarding a network path with CTE.
- If you want to access the FileTables from multiple remote systems, you must install CTE agent on those systems and apply the GuardPoints.



CAUTION

LDT is not supported with SQL FileTables. Only use offline Data Transformation to transform the initial SQL data.

Advantages

- System administrator cannot see the data locally on the SQL server because no CTE Agent is installed on the SQL server.
- The data transferring between servers is also encrypted.

Supported FileTables Use Cases

CTE supports the following FileTables use cases:

CTE Data Transformation of existing files in FileTables

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the FileTable folder for the existing FileTable.
3. Create an offline Data Transformation policy and apply to the GuardPoint on the FileTable folder.
4. Run the Dataxform utility to transform the data.

Protect files in SQL FileTables with CTE

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the FileTable folder for the existing FileTable.
3. Create a production policy and apply the GuardPoint on the FileTable folder.
4. Once the GuardPoint is active, you can use the file table to load and access files.

Protect files with SQL AlwaysOn Availability Groups with CTE

When the database that contains the FILESTREAM, or FileTable data, belongs to an AlwaysOn availability group, the FILESTREAM and FileTable functions accept or return virtual network names (VNNs) instead of computer names.

Configuration guidelines:

1. Install CTE agent on the remote server.
2. Create a new FileTable, or Identify the virtual network names (VNNs) for the existing FileTable.
3. Create a production policy and apply the GuardPoint to the VNN name
4. Once the GuardPoint is active, you can use the FileTable to load and access files.
5. When you enable FILESTREAM on an instance of SQL Server, it creates an instance-level share to provide access to the FILESTREAM data. Access this share by using the computer name in the following format:

```
\\<computer_name>\<filestream_share_name>
```

6. In an AlwaysOn availability group, the computer name is virtualized by using a Virtual Network Name, (VNN). When the computer is the primary replica in an availability group, and databases in the availability group contain FILESTREAM data, then SQL creates a VNN-scoped share to provide access to the FILESTREAM data. Applications that use the file system APIs have to use the VNN-scoped share, which has a path in the following format:

```
\\<VNN>\<filestream_share_name>
```

Install CTE on remote systems and guard the SQL Server VNN names

In this use case, CTE is installed on the SQL administrator system (a separate system from where the SQL Server resides) and a GuardPoint is applied to the VNN name.

Unsupported FileTables Use Cases

CTE does not support the following use cases:

1. Install CTE agent on the SQL Server and locally apply the GuardPoint on the SQL Server storage.
2. Access FileTables with Transact-SQL.
3. Access FileTables with File I/O APIs on the SQL server. Perform all file I/O on the remote system running the CTE agent.

Installing CTE on Microsoft SQL AlwaysOn

This section describes how to implement CTE with Microsoft SQL AlwaysOn in a variety of configurations for primary and secondary replica servers, and assumes that you have a basic understanding of Microsoft SQL database.

You may want to keep the primary server decrypted to serve all users, and use the secondary database for running reports or backups.

- If the database is encrypted, then the Volume Shadow copy-related backups will snapshot and backup encrypted protected data.
- Administrators with the `apply_key` permission can run a query and pull down reports from the secondary

database server without affecting the performance of the primary database server.

- The secondary server could be in a remote Data Recovery location. You may want to secure it with encryption.
- LDT is supported with SQL AlwaysOn. See ["Using LDT with SQL AlwaysOn" on page 67](#) for more information.

Methods for Initial Encryption

There are multiple methods for performing the initial encryption of the databases. Decide on which of the following methods best fits your environment. For more information on transforming data, see the *CTE-Live Data Transformation with Data Security Manager*.

- Data Transformation – Encrypt data in place
- Backup and Restore to a GuardPoint
- Copy and paste the data into a GuardPoint

Configuration 1

- Databases on primary server and secondary replica servers require encryption
- Database name and location of secondary replica server are the same as the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Change the primary database to offline mode.
3. Confirm the creation of a data transformation and/or operational policy.
4. Guard the folder containing the primary database files with that policy:
 - a. If using 'Encrypt data in place' as the selected method of encryption, execute the data transformation and then apply the operational policy.
 - b. If using the 'Copy/Restore' method of encryption, apply the operational policy on an empty folder/device.
5. On the secondary server, create a new folder to store the replicated database.

Note: The folder name and the path must be the same as the primary server.
6. Guard the folder with the operational policy.
7. Perform step 4 above for additional secondary server(s).
8. Put the primary database back into online mode.
9. Setup SQL AlwaysOn High Availability group to perform FULL Data Synchronization.
This copies the primary database and replicates it to secondary replica servers.
10. Verify that the databases in the secondary server are in "Synchronized" mode.

Configuration 2

- Database on the primary server does not require encryption, but the secondary replica database requires it
- Database names and locations for the secondary replica servers are the same as the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Confirm the creation of a data transformation and/or operational policy.
3. On the secondary server, create a new folder to store the replicated database.

Note: The folder name and the path must be the same as the primary server.

4. Guard the folder with the operational policy.
5. Perform step 3 & 4 above for additional secondary server(s).
6. Setup SQL AlwaysOn High Availability group to perform **FULL Data Synchronization**.
This copies the primary database and replicates it to secondary replica servers.
7. Verify that the databases in the secondary server are in “Synchronized” mode.

Configuration 3

- Databases on the primary and secondary replica servers require encryption
- Database name is the same, but the location of the secondary replica server is in a different location from that of the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Change the primary database to offline mode.
3. Confirm the creation of a data transformation and/or operational policy.
4. Guard the folder containing the primary database files with that policy:
 - a. If using 'Encrypt data in place' as the selected method of encryption, execute the data transformation and then apply the operational policy.
 - b. If using the 'Copy/Restore' method of encryption, apply the operational policy on an empty folder/device.
5. On the secondary server, create a new folder to store the replicated database.

Note: The folder name and the path must be the same as the primary server.

6. Guard the folder with the encryption policy.
7. From secondary server, perform the restore to the primary database.
 - a. Select the options **Restore with norecovery** and **Relocate all files to folder**.
 - b. Specify the path of the new folder from step 5.
8. Repeat steps 4 & 5 above for any additional secondary server(s).
9. Setup SQL AlwaysOn High Availability group to perform **JOIN ONLY Data Synchronization**.
This joins the secondary database to the SQL Always High Availability Group. It also establishes replication of new data and logs from the primary to the secondary replicated server.
10. Verify that the databases in the secondary server are in **Synchronized** mode.

Configuration 4

- Database on the primary server does not require encryption, but the secondary replica database requires encryption
- Database name is the same, but the location on the secondary replica server is in a different location than that of the primary server

To perform the procedure:

1. Perform a full backup of the primary database.
2. Confirm the creation of a data transformation and/or operational policy.
3. On the secondary server, create new folder to store the replicated database.
4. Guard the folder with the operational policy.
5. From secondary server, perform restore the primary database:
 - a. Select the options **Restore with norecovery** and **Relocate all files to folder**.
 - b. Specify the path of the new folder from step.
6. Setup SQL AlwaysOn High Availability group to perform **JOIN ONLY Data Synchronization**. Joins the secondary database to the SQL Always HA Group. It also establishes replication of new data and logs from the primary to the secondary replicated server.
7. Verify that the databases in the secondary server are in **Synchronized** mode.

Configuration 5

Following is an alternative method for protecting data in a MS SQL Server AlwaysON environment.

To perform the procedure:

1. Shut down SQL services completely, on the secondary node.

Note: It is important to shut down the secondary node first, in order to keep the assignments the same.

2. Shut down SQL services completely on the primary node.
3. Create GuardPoints, using Data Transformation policies, on the directories containing the databases to be encrypted in the primary node.

Note: Perform encrypt-in-place encryption on each directory.

4. Create GuardPoints, using Data Transformation policies, on the directories containing the databases to be encrypted in the secondary node.

Note: Perform encrypt-in-place encryption on each directory.

5. Delete the GuardPoints, using Data Transformation policies, from the primary node.
6. Create GuardPoints, using operational policies, on the four directories in the primary node.
7. Delete GuardPoints, using Data Transformation policies, from the secondary node.

8. Create GuardPoints, using operational policies, on the four directories in the secondary node.
9. Activate SQL services on the primary node.
10. Activate SQL services on the secondary node.

Data Transformation (Encryption in place)

For more information on transforming and encrypting data-in-place, see the *CTE-Live Data Transformation with Data Security Manager*.

Copy/Restore

For more information on transforming data using the copy and replace method, see the *CTE Data Transformation Guide*.

SQL Server Policy Tuning

In this section, you created and defined a process set for SQL Server that grants certain executables –in this case `sqlservr.exe`– unrestricted access to the database files. The need may arise to allow other executables, and/or users, access to the files.

You can grant this access by:

- Adding to the existing process set
- Creating a new one

The best option depends on the access requirements. The key decision is whether or not to select the **Apply Key** effect along with **Permit** or not. Omitting **Apply Key** on a security rule that still contains **Permit** allows the specified user or process to access to the data, but does not apply the encryption key, so therefore only shows them the data in its encrypted, cypher-text format. This is useful for anti-virus or backup software that may need to scan or copy the file, but does not necessarily need to see the contents.

Using LDT with SQL AlwaysOn

To guard a directory with an LDT (Live Data Transformation) policy, you must temporarily close all of the files in that directory. In an SQL Server AlwaysOn environment, this may entail temporarily stopping the SQL Server service on the node that is being guarded. Once the directory is guarded, then you can start the SQL Server service immediately.

It is important to remember that the SQL Server AlwaysOn replication standard operating procedures.

- If one SQL Server service is taken offline for any reason, then once it is brought back on line, it takes the SQL Server a moment to re-synchronize the database nodes.
- The longer that secondary service was down, and the more inserts/updates and deletes that occurred on the still active node during that downtime, then the longer the synchronization period takes.
- During that synchronization period, any attempted fail over results in the SQL Server warning that data loss may occur if the fail over continues. However, once the SQL Server has completed re-synchronizing that secondary node, then any fail over is safe and does not result in loss of data.

Chapter 7: CTE with DFSR

The Microsoft Distributed File System Replication (DFSR) service is a multi-master replication engine used to keep folders synchronized on multiple servers. Using CTE with DFSR requires some special configuration to make sure that all folders within a GuardPoint are only encrypted once, and that all sources to which those folders are replicated can access the proper encryption key to read the encrypted data.

For details about DFSR, see the Microsoft DFSR documentation at [Distributed File System Replication](#).

This section contains the following topics:

Overview	68
Creating Required DFSR Policy Components	70
Using the Standard Encryption Method	74
Using the CTE-LDT Encryption Method	84

Overview

How you deploy CTE in a DFSR environment depends on the topology you have chosen for your DFSR configuration. Microsoft offers several topology options for DFSR:

- **Hub and Spoke.** In this configuration, there is a central server (the hub) whose contents is replicated on multiple satellite servers (the spokes). While each spoke server has a two-way communication channel with the hub server, none of the spoke servers can communicate with each other. If the data changes on one spoke server, that server communicates the changes back to the hub server and the hub server initiates the data replication on all other spoke servers.

This configuration allows you to encrypt servers one at a time, starting with the hub and then moving outwards to the spokes.

- **Full Mesh.** In this configuration, any server in the mesh has a two-way communication channel with every other server in the mesh, and data replication can be initiated by any server on all the other servers.

In this configuration, you must stop the replication service while you encrypt the data on all servers in the mesh. You cannot restart the replication service until the initial encryption has completed on all servers.

CTE Encryption Methods

CTE supports two encryption methods:

- Standard offline data transformation, where the data is unavailable while it is being encrypted or rekeyed.
- Live data transformation, where the data is encrypted and rekeyed in the background while it remains accessible to users. This method requires a separate license for the CTE-LDT feature.

While DFSR policies have some unique required components, the basic policy and GuardPoint creation process is identical to non-DFSR environments. For details about offline data transformation, see the *CTE Data Transformation Guide*. For details about CTE-LDT, see the *CTE-Live Data Transformation with Data Security Manager* or *CTE-Live Data Transformation with CipherTrust Manager*.

Considerations with DFSR

If you are using CTE in a DFSR environment, keep in mind the following:

- You should always back up your data prior to beginning the encryption process and you should have a full backup of the data in the hub server before you restore a spoke.
- You cannot place a GuardPoint *anywhere* on the boot drive, so if your DFSR replication point is currently `C:\`, or a directory under `C:\` such as `C:\data\`, you need to move that data and its replication point to a new volume on the server before you can encrypt it.
- If you are backing up your DFS data, make sure that your backup software is *not* backing up the archive bit. File replication gets triggered by file version change or a modified time stamp. As such, there is a chance that updating the archive bit may cause issues that trigger a replication storm, which will then put a heavy encryption load on the servers.
- You must add the CTE GuardPoint at or above the level of the DFSR replication point. For example:
 - If the replication point is `D:\`, the CTE GuardPoint must also be at `D:\`. Adding a GuardPoint on a directory in `D:\`, such as `D:\data\`, will fail.
 - If the replication point is `D:\data\`, you can add a GuardPoint at `D:\data\` or `D:\`, but you *cannot* add a GuardPoint on a subdirectory of `D:\data\` such as `D:\data\HR-files\`.
- When you set a replication point, Microsoft automatically creates a private directory called `<dir name>\DfsrPrivate` that goes with that replication point. For example, if the replication point is set on `D:\`, the private directory would be `D:\DfsrPrivate`. If the replication point is set on `D:\data\`, the private directory would be `D:\data\DfsrPrivate`.

How this private directory must be handled depends on the the encryption method that you are using.

- For Standard encryption, you must guard the private directory with the same policy that you use for the main GuardPoint. If the GuardPoint is at the root of the volume (for example, `D:\`), this happens automatically. But if you are guarding a specific directory, such as `D:\data\`, you need to create a second GuardPoint using the same policy on `D:\data\DfsrPrivate`. For details, see ["Creating Standard GuardPoints with the DFSR Hub and Spoke Topology" on page 80](#) or ["Creating Standard GuardPoints with the DFSR Full Mesh Topology" on page 83](#).
- For live data transformation, you must guard the private directory with the same policy that you use for the main GuardPoint, even if the GuardPoint is at the root level. (For example, you must have a GuardPoint for both `D:\` and `D:\DfsrPrivate\`.) In addition, you must exclude this directory from CTE-LDT processing. For details, see ["Creating a CTE-LDT GuardPoint for DFSR" on page 87](#).
- The policy you specify for a DFSR GuardPoint *cannot* contain a resource set in any of the key rules included in the policy. All files in the guarded directory and its subdirectories must be encrypted with the same encryption key *without exception*. Additionally, if you rekey the GuardPoint, all files must be rekeyed with the same encryption key.
- If you want to change from one encryption key to an entirely different encryption key (as opposed to rekeying the data with a new version of the existing key), you must decrypt the data and remove all existing GuardPoints so that you have a clean environment. Then you can start the CTE encryption process over from the beginning. You cannot change from one encryption key to another if any of the existing data is still encrypted with the old key. If you attempt to do so, you may encounter data replication errors and you may need to delete the entire volume and recreate it.
- When CTE encrypts data on a node, the encrypted data must be replicated to other nodes in the configuration. This may result in increased replication activity on the network.

CTE Configuration Workflow

In order to configure CTE with DFSR, you must complete the following tasks:

Step	Description
1	Identify the volumes or folders you intend to encrypt.
2	Make sure you have a good backup of the data you intend to encrypt.
3	Select an encryption method and make sure you understand how to create and deploy CTE GuardPoints using that encryption method. For details, see one of the following documents: <ul style="list-style-type: none">• <i>CTE Data Transformation Guide</i>• <i>CTE-Live Data Transformation with CipherTrust Manager</i>• <i>CTE-Live Data Transformation with Data Security Manager</i>
4	Create a DFSR Process Set and User Set for the policy. For details, see " Creating Required DFSR Policy Components " below.
5	Create the policies and GuardPoints you need to protect your data, using the process appropriate to the selected encryption method. For details, see one of the following: <ul style="list-style-type: none">• "Using the Standard Encryption Method" on page 74• "Using the CTE-LDT Encryption Method" on page 84

Creating Required DFSR Policy Components

DFSR uses two services to for the replication process, `dfsrs.exe` and `ntoskrnl.exe` that must be associated with the NT AUTHORITY user. In order to do this, you need to create a process set and a user set that must then be combined into a security rule in the policy.

How you do this depends on the key manager that you are using.

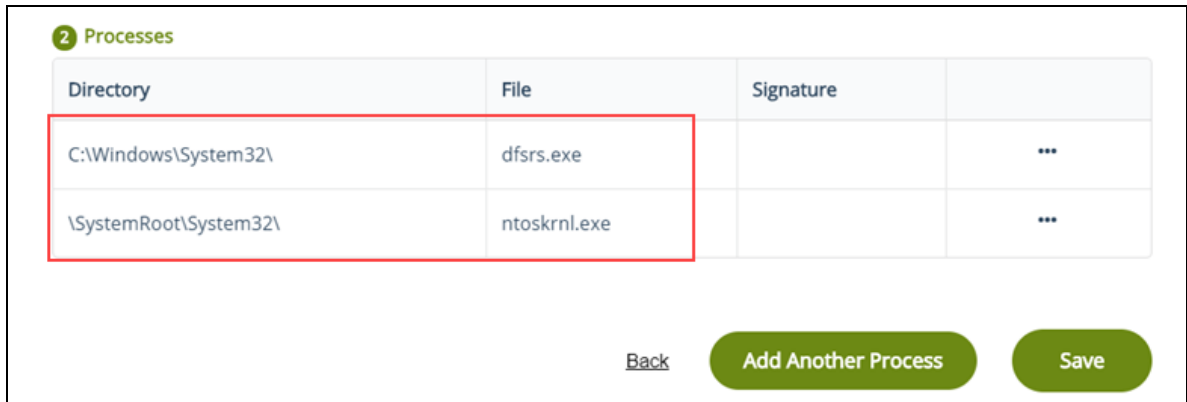
Note

Once you create these components, you can use them in any number of policies for both standard and CTE-LDT GuardPoints.

Process Using CipherTrust Manager

1. Log into the CipherTrust Manager Console and switch to the correct domain if required.
2. Launch the **Transparent Encryption** application.
3. In the left-hand menu bar, expand **Policies** and select **Policy Elements**.

4. Create a process set for the required DFSR processes:
 - a. Click the **Process Sets** tab.
 - b. Click **Create Process Set**.
 - c. In the **Name** field, enter a name for this process set. In this example, we will use `DFSR-Processes`.
 - d. Click **Next**.
 - e. Enter the first DFSR process:
 - In the **Directory** field, enter `C:\Windows\System32\`.
 - In the **File** field, enter `dfsrs.exe`.
 - f. Click **Next**.
 - g. Below the table, click **Add Another Process**:
 - In the **Directory** field, enter `\SystemRoot\System32\`.
 - In the **File** field, enter `ntoskrnl.exe`.
 - h. Click **Next**. The process set should look like this:



- i. Click **Save** to save the process set.

5. Create the user set for the required NT AUTHORITY user:
 - a. Click the **User Sets** tab.
 - b. Click **Create User Set**.
 - c. In the **Name** field, enter a name for the user set. In this example we will use `Local_NT_AUTHORITY`.
 - d. Click **Next**.
 - e. Click the **Manually Add Users** tab.
 - f. In the **uname** field, enter `SYSTEM`.
 - g. In the **OS domain** field, enter `NT AUTHORITY`.
 - h. Click **Next**. The user set should look like this:

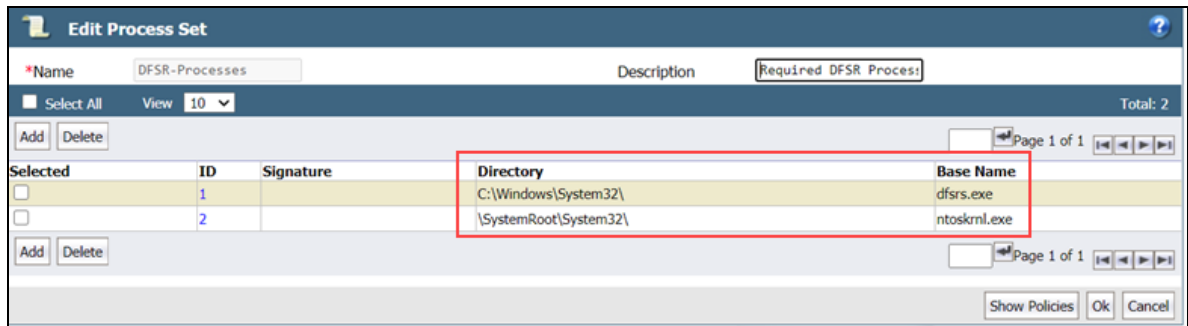


uname	UID	gname	GID	OS domain	
SYSTEM				NT AUTHORITY	<input type="button" value="Remove"/>

- i. Click **Save** to save the user set.
 - j. Optionally create another user set for other authorized users in the namespace. For example, you may want to add the "Administrator" user in each of the domains that are part of the namespace. You can create as many separate user sets as required.
6. When you have finished created the required components, you can use those components to create your policies and GuardPoints. How you do so depends on which encryption method you are using. For details, see one of the following:
 - ["Using the Standard Encryption Method" on page 74](#)
 - ["Using the CTE-LDT Encryption Method" on page 84](#)

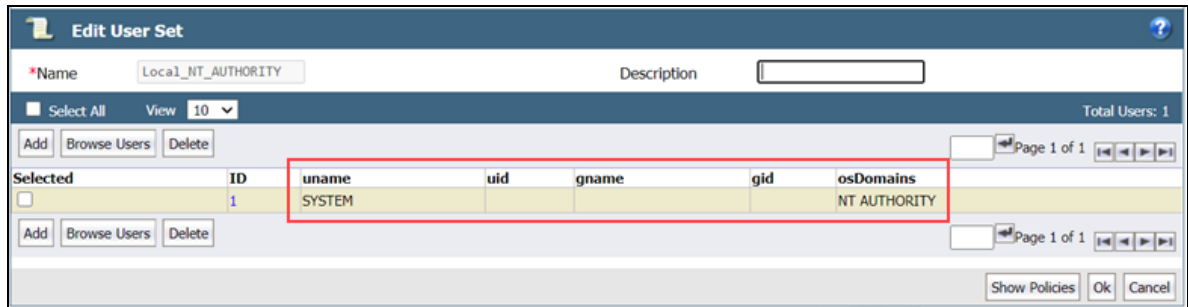
Process Using the DSM

1. Log into the DSM Management Console and switch to the domain you want to use.
2. In the top menu bar, click **Policies > Manage Policies > Process Sets**.
3. Create a process set for the required DFSR processes:
 - a. In the table, click **Add**.
 - b. In the Name field, enter a name for this process set. In this example, we will use `DFSR-Processes`.
 - c. In the table, click **Add** and enter the first DFSR process:
 - In the Directory field, enter `C:\Windows\System32\`.
 - In the File field, enter `dfsrs.exe`.
 - d. Click **Ok**.
 - e. In the table, click **Add** again to enter the second required process:
 - In the Directory field, enter `\SystemRoot\System32\`.
 - In the File field, enter `ntoskrnl.exe`.
 - f. Click **Ok**. The process set should now look like this:



- g. Click **Ok** to save the process set.
4. In the top menu bar, click **Policies > Manage Policies > User Sets**.

5. Create the user set for the required NT AUTHORITY user:
 - a. In the table, click **Add**.
 - b. In the **Name** field, enter a name for the user set. In this example we will use `Local_NT_AUTHORITY`.
 - c. In the table, click **Add**.
 - d. In the **uname** field, enter `SYSTEM`.
 - e. In the **osDomains** field, enter `NT AUTHORITY`.
 - f. Click **Ok**. The user set should look like this:



- g. Click **Ok** to save the user set.
 - h. Optionally create another user set for other authorized users in the namespace. For example, you may want to add the "Administrator" user in each of the domains that are part of the namespace. You can create as many separate user sets as required.
6. When you have finished created the required components, you can use those components to create your policies and GuardPoints. How you do so depends on which encryption method you are using. For details, see one of the following:
 - ["Using the Standard Encryption Method" below](#)
 - ["Using the CTE-LDT Encryption Method" on page 84](#)

Using the Standard Encryption Method

If you want to encrypt your data using the standard (offline) encryption method, you need to create two different policies. The first policy is the initial encryption policy that specifies the symmetric key you want to use to encrypt the data for the first time. The second is the production policy that you want to use for day-to-day operations on the encrypted data.

The initial encryption must be done while the volume or directory is offline, and users and applications must be prevented from accessing the data until the entire encryption process has finished. Once this initial encryption has been completed, any new or changed data in the GuardPoint will be automatically encrypted as it is added.

Note

If you want to encrypt the data without restricting access during the encryption process, you can use the CTE-LDT feature. For details, see ["Using the CTE-LDT Encryption Method" on page 84](#).

To use the standard encryption method:

1. Make sure you have created the required policy components for DFSR as described in ["Creating Required DFSR Policy Components" on page 70](#).
2. Create the initial encryption and production policies as described in ["Creating Standard Policies for DFSR" on the next page](#).

3. Create the GuardPoints you want to use. The GuardPoint creation method depends on your DFSR topology. For details, see one of the following:
 - ["Creating Standard GuardPoints with the DFSR Hub and Spoke Topology" on page 80](#)
 - ["Creating Standard GuardPoints with the DFSR Full Mesh Topology" on page 83](#)

Creating Standard Policies for DFSR

If you are using the standard (offline) data encryption option, you need to create two policies, a data transformation policy that is used for the initial encryption and an operational policy that is used for day-to-day access of the encrypted data. The initial encryption policy is identical to the one you use for any standard GuardPoint. It is the operational policy that has DFSR-specific requirements.

How you create policies for DFSR depends on the key manager that you are using.

Procedure Using CipherTrust Manager

1. Log into the CipherTrust Manager Console and switch to the correct domain if required.
2. If you do not know which symmetric key you want to use to encrypt the data or you want to create a new key to use for the DFSR namespace, launch the Keys & Access Management application and locate an existing symmetric key or create a new symmetric key. For details on creating a symmetric key for standard encryption, see the *CTE Data Transformation Guide*.
3. Launch the **Transparent Encryption** application.
4. In the left-hand menu bar, click **Policies**.
5. To create the initial data encryption policy, click **Create Policy** and enter the following information.

Note: The following example assumes you are using `dataxform` to encrypt the data in place. If you are using the copy or restore encryption method, create your initial data transformation policy as described in the *CTE Data Transformation Guide*.

- a. In the **Name** field, enter a name for the policy. This example uses `DFSR-Std-Initial`.
- b. In the **Policy Type** field, select **Standard**.
- c. Enable the **Data Transformation** option.

Name *
DFSR-Std-Initial

Policy Type
Standard

Description

Learn Mode:

Data Transformation:

- d. Click **Next**.
- e. On the Security Rules page, make sure there is a security rule with the action **key_op** and the effect **permit,applykey**. If CipherTrust Manager did not add this security rule automatically, go back to the General Info page and make sure that the **Data Transformation** option is enabled.
- f. On the Security Rules page, click **Create Security Rule** and add another security rule that prevents any other process from accessing the data while it is being encrypted:
 - In the **Action** field, click **Select** and choose `all_ops`.
 - In the **Effect** field, click **Select** and choose `Deny`.

When you are done, click **Add** to save the security rule.

Resource Set	User Set	Process Set	Action	Effect	Browsing	
			key_op	permit,applykey	Yes	...
			all_ops	deny	Yes	...

- g. Click **Next**.

- h. On the Key Rules page, click **Create Key Rule**. In the **Current Key Name** field, click **Select** and choose `clear_key`.



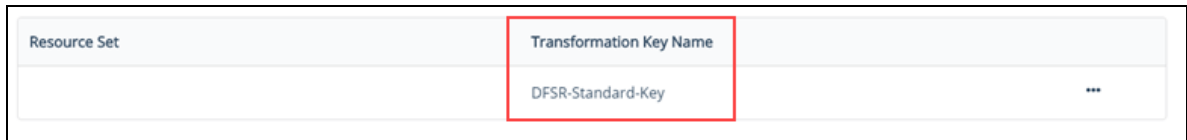
The screenshot shows a dropdown menu for 'Current Key Name' with 'clear_key' selected. The menu is highlighted with a red box. To the left, the 'Resource Set' field is visible. To the right, there are three dots indicating more options.



CAUTION

In a DFSR environment, you *must* apply the initial encryption policy on unencrypted data **ONLY** (the current key must be set to `clear_key`). If your data is already encrypted, you must decrypt it and completely remove the existing GuardPoint before re-encrypting the data with a new key from scratch. For details, see "[Considerations with DFSR](#)" on page 69.

- i. Click **Add** to save the key rule.
- j. Click **Next**.
- k. On the Data Transformation page, click **Create Data Transformation Rule**. In the **Transformation Key Name** field, click **Select** and choose the symmetric key you want to use for data transformation.
- l. Click **Add** to save the data transformation rule.



The screenshot shows a dropdown menu for 'Transformation Key Name' with 'DFSR-Standard-Key' selected. The menu is highlighted with a red box. To the left, the 'Resource Set' field is visible. To the right, there are three dots indicating more options.

- m. Click **Next**.
- n. Verify the policy information and click **Save** to save the initial encryption policy.

6. To create the production policy, **Create Policy** and enter the following information.
 - a. In the **Name** field, enter a name for the policy. This example uses `DFSR-Std-Policy`.
 - b. In the **Policy Type** field, select **Standard**.
 - c. Click **Next**.
 - d. On the Security Rules page, click **Create Security Rule** and add the following security rule:
 - In the **User Set** field, click **Select** and choose the user set you created that contains NT AUTHORITY. For details, see ["Creating Required DFSR Policy Components" on page 70](#).
 - In the **Process Set** field, click **Select** and choose the process set you created that contains the required DFSR processes `dfsrs.exe` and `ntoskrnl.exe`.
 - In the **Effect** field, click **Select** and choose **Permit and Audit**.
 - e. Click **Add**.

Resource Set	User Set	Process Set	Action	Effect	Browsing
	Local_NT_AU...	DFSR-Processes		permit,audit	Yes ...

- f. Add any other security rules you need to your policy. When you have added all your security rules, click **Next**.
- g. On the Key Rules page, click **Create Key Rule**. In the **Current Key Name** field, click **Select** and choose the symmetric key you used to encrypt the data in the initial data encryption policy.

Resource Set	Key Name
	DFSR-Standard-Key ...

- h. Verify the policy information and click **Save** to save the production policy.
7. When you have both policies ready, you can create the required DFSR GuardPoints as described in ["Creating Standard GuardPoints with the DFSR Hub and Spoke Topology" on page 80](#) or ["Creating Standard GuardPoints with the DFSR Full Mesh Topology" on page 83](#).

Procedure Using the DSM

1. Log into the DSM Management Console and switch to the domain you want to use.
2. If you do not know which symmetric key you want to use to encrypt the data or you want to create a new key to use for the DFSR namespace, in the top menu bar click **Keys** and locate an existing symmetric key or create a new symmetric key. For details on creating a symmetric key for standard encryption, see the *CTE Data Transformation Guide*.
3. In the top menu bar, click **Policies**.
4. To create the initial data encryption policy, in the Policies table, click **Add** and enter the following information.

Note: The following example assumes you are using `dataxform` to encrypt the data in place. If you are using the copy or restore encryption method, create your initial data transformation policy as described in the *CTE Data Transformation Guide*.

- a. In the **Policy Type** field, select **Standard**.
- b. In the **Name** field, enter a name for the policy. This example uses `DFSR-Std-Initial`.
- c. In the Security Rules table, click **Add** and add the following security rule that allows the data to be encrypted:
 - In the **Action** field, select or enter `key_op`.
 - In the **Effect** field, select or enter `Permit, Apply Key`.
- d. Click **Ok**. When you add the `key_op` rule, the DSM displays the Data Transformation Rules area.
- e. In the Security Rules table, click **Add** and another security rule that prevents any other process from accessing the data while it is being encrypted:
 - In the **Action** field, select or enter `all_ops`.
 - In the **Effect** field, select or enter `Deny`.

Select	Order	Resource	User	Process	Action	Effect	When	Browsing
<input type="checkbox"/>	1				key_op	Apply Key, Permit		Yes
<input type="checkbox"/>	2				all_ops	Deny		Yes

- f. In the Key Selection Rules table, click **Add** and select `clear_key` in the **Key** field.
- g. Click **Ok** to add the key rule.

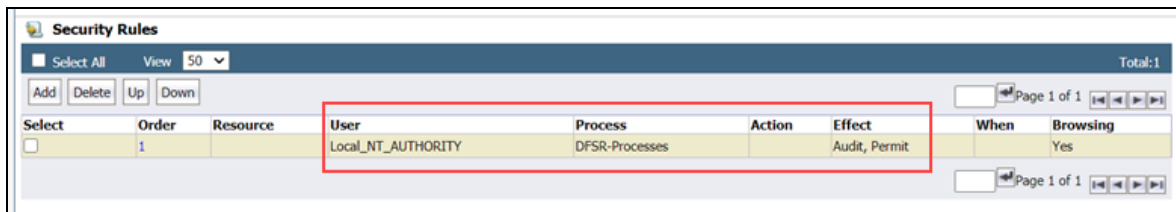
Select	Order	Resource	Key
<input type="checkbox"/>	1		clear_key

- h. In the Data Transformation Rules table, click **Add** and select the symmetric key you want to use for data encryption in the **Key** field.
- i. Click **Ok** to add the data transformation rule.

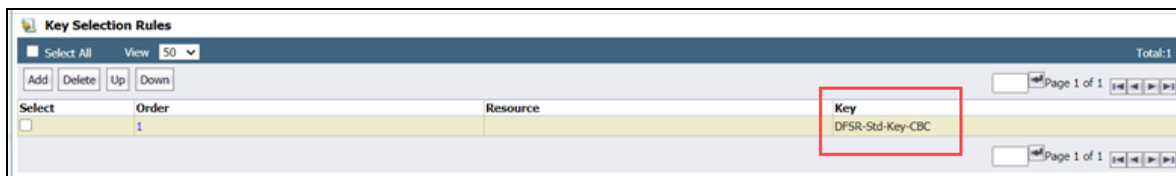
Select	Order	Resource	Key
<input type="checkbox"/>	1		DFSR-Std-Key-CBC

- j. Click **Ok** to save the initial encryption policy.

5. To create the production policy, in the Policies table, click **Add** and enter the following information.
 - a. In the **Policy Type** field, select **Standard**.
 - b. In the **Name** field, enter a name for the policy. This example uses `DFSR-Std-Pol`.
 - c. In the Security Rules table, click **Add** and add the following security rule:
 - In the **User** field, select the user set you created that contains NT AUTHORITY. For details, see ["Creating Required DFSR Policy Components" on page 70](#).
 - In the **Process** field, select the process set you created that contains the required DFSR processes `dfsrs.exe` and `ntoskrnl.exe`.
 - In the **Effect** field, select or enter `Permit, Audit`.
 - d. Click **Ok**.



- e. Add any other security rules you need to your policy.
- f. When you have finished adding security rules, add a key selection rule by clicking **Add** in the Key Selection Rules Table. In the **Key** field, select the symmetric key you used to encrypt the data in the initial data encryption policy and click **Ok**.



- g. Click **Ok** to save the production policy.
6. When you have both policies ready, you can create the required DFSR GuardPoints as described in ["Creating Standard GuardPoints with the DFSR Hub and Spoke Topology" below](#) or ["Creating Standard GuardPoints with the DFSR Full Mesh Topology" on page 83](#).

Creating Standard GuardPoints with the DFSR Hub and Spoke Topology

If you are using the hub and spoke DFSR topology, you should start encrypt the data on the hub and then encrypt the data on the spokes. After you have encrypted the data on the hub server, you have two options for the data on the spoke servers:

- **Option 1: Delete the existing spoke server data and allow DFSR to replicate the encrypted hub data to the spoke servers.** The advantage of this method is that you only need to encrypt the data on the hub. The disadvantage is that it will take time to replicate the data on all the spoke servers.
- **Option 2: Encrypt each spoke server using the same encryption process as you use on the hub server.** The advantage of this method is that you do not need to wait for the full data replication process across the network. The disadvantage is that you must run the encryption process on all spoke servers.

Prerequisites

- Make sure you have a good backup of the data you plan to encrypt.
- Make sure you know what devices or directories you plan to protect.
- Make sure you understand how data transformation GuardPoints are created as described in the *CTE Data Transformation Guide*.
- Make sure you have an initial encryption and a production policy as described in ["Creating Standard Policies for DFSR" on page 75](#).

Note

The following procedures assume you are using `dataxform` to encrypt the data in place. If you are using the copy or restore encryption method, see the *CTE Data Transformation Guide*.

Procedure for Option 1: Use DFSR to Replicate the Encrypted Data

1. Disable user and application access to all devices and directories you intend to encrypt so that no users can add or change the data during the transformation process. This must be done on the hub server and all spoke servers in the namespace.

Note

You do *not* have to take down the namespace itself.

2. On the hub server:
 - a. Stop the DFSR service.
 - b. In your key manager, create the GuardPoints you want to encrypt and apply the initial encryption policy to those GuardPoints.

Make sure that all GuardPoints are at or above the level of the DFSR replication point as described in ["Considerations with DFSR" on page 69](#).

Note: Do not create GuardPoints for the `DfsrPrivate` directories yet.

- c. On the hub server, run the `dataxform` utility as described in the *CTE Data Transformation Guide*.
- d. After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and regard them using the production DFSR policy.
- e. If any of your GuardPoints are at the directory level, create a GuardPoint for the `<dir name>\DfsrPrivate` directory that goes with that GuardPoint. For example, if the GuardPoint is `D:\data\`, the private directory would be `D:\data\DfsrPrivate`. Make sure you use the same production policy for the `DfsrPrivate` directory that you used for the main directory.



WARNING

Do not start the DFSR service yet.

3. On each spoke server, do the following:
 - a. Stop the DFSR service on the spoke server.
 - b. Delete the data in all devices and directories that you added GuardPoints for on the hub server.
 - c. In your key manager, create the same GuardPoints on the spoke server that you created on the hub server, making sure that you apply the same operational policy to each GuardPoint on the spoke server that you applied on the hub server.

Make sure you also create the same `DfsrPrivate` GuardPoints on the spoke server that you created on the hub server.

Note

Because the directories are empty, you do not need to use the initial encryption policy or the `dataxform` utility on the spoke servers. You can just guard the empty directory and the private directories directly using the production policy.

- d. Start the DFSR service on the spoke server.
4. Repeat the previous step for each spoke server in the configuration.
5. When every spoke server has the exact same production GuardPoints as the hub server, return to the hub server and do the following:
 - a. Start the DFSR service on the hub.
 - b. Force replication from the hub to the spokes.
6. When replication is complete to all spokes in the configuration, re-enable user and application access to the devices and directories you encrypted.

Procedure for Option 2: Encrypt the Data on All Servers

1. Disable user and application access to all devices and directories you intend to encrypt so that no users can add or change the data during the transformation process. This must be done on the hub server and all spoke servers in the namespace.

Note

You do *not* have to take down the namespace itself.

2. On the hub server, do the following:
 - a. Disable access to the hub server so that no one can change the data during the transformation process.
 - b. Stop the DFSR service on the hub.
 - c. In your key manager, create the GuardPoints you want to encrypt and apply the initial encryption policy to those GuardPoints.

Make sure that all GuardPoints are at or above the level of the DFSR replication point as described in ["Considerations with DFSR" on page 69](#).

Note: Do not create GuardPoints for the `DfsrPrivate` directories yet.

- d. Run the `dataxform` utility on the hub server as described in the *CTE Data Transformation Guide*.
 - e. After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and reguard them using the production DFSR policy.
 - f. If any of your GuardPoints are at the directory level, create a GuardPoint for the `<dir name>\DfsrPrivate` directory that goes with that GuardPoint. For example, if the GuardPoint is `D:\data\`, the private directory would be `D:\data\DfsrPrivate`. Make sure you use the same production policy for the `DfsrPrivate` directory that you used for the main directory.
 - g. Restart the DFSR service on the hub server.

3. On each spoke server, do the following:
 - a. Stop the DFSR service on the spoke server.
 - b. In your key manager, create the same GuardPoints on the spoke server that you created on the hub server, making sure that you apply the same initial encryption policy to the GuardPoints on the spoke server that you applied on the hub server.
Do not create the `DfsrPrivate` GuardPoints yet.
 - c. On the spoke server, run the `dataxform` utility as described in the *CTE Data Transformation Guide*.
 - d. After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and reguard them using the same production DFSR policy that you used for the corresponding GuardPoint on the hub server.
 - e. Create the same `DfsrPrivate` GuardPoints on the spoke server that you created on the hub server. Make sure you use the same production policy for the `DfsrPrivate` directory that you used for the main directory.
 - f. Restart the DFSR service on the spoke server.
 - g. Re-enable user and application access to the spoke server.
4. Repeat the previous step for each spoke server in the configuration.
5. When data encryption is complete to all spokes in the configuration, re-enable user and application access to the devices and directories you encrypted.

Creating Standard GuardPoints with the DFSR Full Mesh Topology

If you are using the full mesh DFSR topology, you must restrict access to the data on all servers in the namespace until it has been encrypted on all servers in the namespace. That means the data will be inaccessible to users and applications until the encryption procedure has been completed on all servers.

Prerequisites

- Make sure you have a good backup of the data you plan to encrypt.
- Make sure you know what devices or directories you plan to protect.
- Make sure you understand how data transformation GuardPoints are created as described in the *CTE Data Transformation Guide*.
- Make sure you have an initial encryption and a production policy as described in "[Creating Standard Policies for DFSR](#)" on page 75.

Note

The following procedure assumes you are using `dataxform` to encrypt the data in place. If you are using the copy or restore encryption method, see the *CTE Data Transformation Guide*.

Procedure

1. On *all* servers in the configuration:
 - Disable user and application access to all devices and directories you intend to encrypt so that no users can add or change the data during the transformation process.
 - Stop the DFSR service on each server.

The DFSR service must be stopped on all servers before you can create the GuardPoints on any server in the configuration.

2. On one of the servers in the configuration, do the following:
 - a. In your key manager, create the GuardPoints you want to encrypt and apply the initial encryption policy to those GuardPoints.

Make sure that all GuardPoints are at or above the level of the DFSR replication point as described in ["Considerations with DFSR" on page 69](#).

Note: Do not create GuardPoints for the `DfsrPrivate` directories yet.

- b. Run the `dataxform` utility on the server as described in the *CTE Data Transformation Guide*.
 - c. After the data encryption process has completed, unguard the GuardPoints that use the initial encryption policy and reguard them using the production DFSR policy.
 - d. If any of your GuardPoints are at the directory level, create a GuardPoint for the `<dir name>\DfsrPrivate` directory that goes with that GuardPoint. For example, If the GuardPoint is `D:\data\`, the private directory would be `D:\data\DfsrPrivate`. Make sure you use the same production policy for the `DfsrPrivate` directory that you used for the main directory.
3. Repeat the previous step for each one of the servers in the configuration.

When you are done, the production GuardPoints should be identical on every server in the namespace.
4. Restart the DFSR service on the each server in the namespace.
5. Re-enable user and application access to all devices and directories.

Using the CTE-LDT Encryption Method

If you want to encrypt your data using the live data transformation encryption method, you need to create a Live Data Transformation policy and use that to create your GuardPoints. All encryption will be done in the background while users continue to access the data.

With CTE-LDT, the data will be automatically rekeyed periodically based on the expiration date and the life span of the versioned key used to encrypt the data.

To use the CTE-LDT encryption method:

1. Make sure you have created the required policy components for DFSR as described in ["Creating Required DFSR Policy Components" on page 70](#).
2. If you do not already have a versioned encryption key, create one as described in *CTE-Live Data Transformation with Data Security Manager* or *CTE-Live Data Transformation with CipherTrust Manager*.
3. Create the Live Data Transformation policy as described in ["Creating a CTE-LDT Policy for DFSR" on the next page](#).
4. Create the GuardPoints you want to use as described in ["Creating a CTE-LDT GuardPoint for DFSR" on page 87](#).

Creating a CTE-LDT Policy for DFSR

How you create policies for DFSR depends on the key manager that you are using.

Procedure Using CipherTrust Manager

1. Log into the CipherTrust Manager Console and switch to the correct domain if required.
2. If you do not know which versioned key you want to use to encrypt the data or you want to create a new key to use for the DFSR namespace, launch the Keys & Access Management application and locate an existing versioned key or create a new versioned key. For details on creating a versioned key for CTE-LDT, see *CTE-Live Data Transformation with CipherTrust Manager*.
3. Launch the **Transparent Encryption** application.
4. In the left-hand menu bar, click **Policies**.
5. Click **Create Policy**.
6. Enter a name for the policy in the **Name** field.
7. In the **Policy Type** field, select **Live Data Transformation**.
8. Click **Next**.
9. On the Security Rules page, make sure there is a security rule with the action **key_op** and the effect **permit,applykey**. If CipherTrust Manager did not add this security rule automatically, go back to the General Info page and make sure that the policy type is set to **Live Data Transformation**.
10. On the Security Rules page, click **Create Security Rule** and add the following security rule:
 - In the **User Set** field, select the user set you created that contains NT AUTHORITY. For details, see ["Creating Required DFSR Policy Components" on page 70](#).
 - In the **Process Set** field, select the process set you created that contains the required DFSR processes `dfsrs.exe` and `ntoskrnl.exe`.
 - In the **Action** field, select `all_ops`.
 - In the **Effect** field, select `Permit`.

When you are done, click **Add** to save the security rule.

Resource Set	User Set	Process Set	Action	Effect	Browsing
▶			key_op	permit,applykey	No
▶	Local_NT_AUTH	DFSR-Processes		permit	Yes ***

11. Add any other security rules you need to your policy. When you are done, click **Next**.

12. On the Key Rules page, click Create Key Rule and add the following key rule:

- In the **Current Key** field, select `clear_key`.



CAUTION

In a DFSR environment, you *must* apply the CTE-LDT policy on unencrypted data **ONLY** (the current key must be set to `clear_key`). If your data is already encrypted, you must decrypt it and completely remove the existing GuardPoint before re-encrypting the data with a new key from scratch. For details, see ["Considerations with DFSR" on page 69](#).

- In the **Transformation Key** field, select the CTE-LDT versioned key you want to use to encrypt the data.

When you are done, click **Add** to save the key rule.

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule	
	clear_key	DRSR-LDT-Key	No	...

13. Click **Next**.

14. Verify the policy information and click **Save** to save the CTE-LDT policy.

Procedure Using the DSM

1. Log into the DSM Management Console and switch to the domain you want to use.
2. Identify an existing versioned CBC or CBC CS1 key you want to use for data transformation or create a new versioned key. For details about creating CTE-LDT versioned keys, see *CTE-Live Data Transformation with CipherTrust Manager* or *CTE-Live Data Transformation with Data Security Manager*.
3. In the top menu bar, click **Policies**.
4. To create the initial data encryption policy, in the Policies table, click **Add** and enter the following information.
 - a. In the **Policy Type** field, select **Live Data Transformation**.

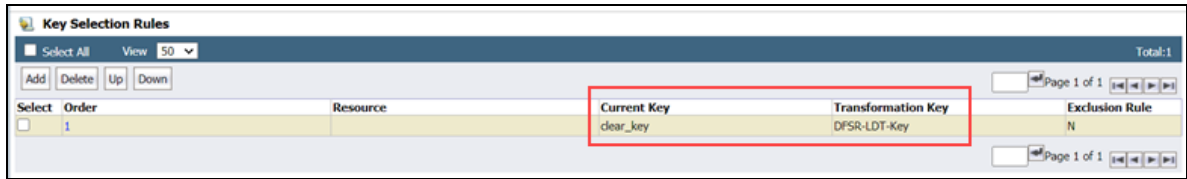
When you select this policy type, the DSM automatically adds the `key_op` security rule to the Security Rules area.

- b. In the **Name** field, enter a name for the policy. This example uses `DFSR-LDT-Policy`.
- c. In the Security Rules table, click **Add** and add the following security rule:
 - In the **User** field, select the user set you created that contains NT AUTHORITY. For details, see ["Creating Required DFSR Policy Components" on page 70](#).
 - In the **Process** field, select the process set you created that contains the required DFSR processes `dfsrs.exe` and `ntoskrnl.exe`.
 - In the **Action** field, select or enter `all_ops`.
 - In the **Effect** field, select or enter `Permit`.
- d. Click **Ok** to add the security rule.

Select	Order	Resource	User	Process	Action	Effect	When	Browsing
<input type="checkbox"/>	1				key_op	Apply Key, Permit		No
<input type="checkbox"/>	2		Local_NT_AUTHORITY	DFSR-Processes	all_ops	Permit		Yes

- e. Add any other security rules you need to your policy.

- f. In the Key Selection Rules table, click **Add** and add the following key rule:
 - In the **Current Key** field, select `clear_key`.
 - In the **Transformation Key** field, select the CTE-LDT versioned key you want to use to encrypt the data.
- g. Click **Ok** to add the key rule.



- h. Click **Ok** to save the CTE-LDT policy.
5. After the CTE-LDT policy has been created, you can create the required DFSR GuardPoints as described in ["Creating a CTE-LDT GuardPoint for DFSR"](#) below.

Creating a CTE-LDT GuardPoint for DFSR

Before you can create a CTE-LDT GuardPoint, you must set CTE-LDT to ignore the DFSR private directory that Microsoft automatically creates when you create a DFSR replication point. The private directory should **not** be encrypted by CTE-LDT.

1. Log into one of the DFSR servers in your network as an administrator.
2. For each GuardPoint you intend to set up on the server, exclude the matching `DfsrPrivate` directory from the CTE-LDT process using the `voradmin ldt exlist add <guard path>` command.

For example, if you are going to guard `D:\data`, `G:\HR Files`, and the entire `F:` drive, you would use the following commands:

```
voradmin ldt exlist add D:\data\DfsrPrivate
voradmin ldt exlist add G:\HR Files\DfsrPrivate
voradmin ldt exlist add F:\DfsrPrivate
```

To make sure CTE-LDT is ignoring the proper directories, use the `voradmin ldt exlist get` command:

```
C:\>voradmin ldt exlist get
```

Live Data Transformation exclusion list. Following GuardPoints will be excluded from the Live Data Transformation.

```
G:\HR Files\DfsrPrivate
D:\data\DfsrPrivate
F:\DfsrPrivate
```

3. Reboot all of the CTE-LDT agent hosts before you create any CTE-LDTGuardPoints.
4. Repeat the previous step on each server in your configuration before you create any CTE-LDT GuardPoints.

5. After you have excluded all `DfsrPrivate` directories on all servers from CTE-LDT processing, log into your key manager and set your CTE-LDT properties. When you begin the initial encryption, Thales recommends that you throttle the CTE-LDT processing speed with a CPU cap of 20%. You can increase this cap as more of the data is encrypted and there are fewer deltas between the DFS staging area and the production area.

How you set the cap depends on the key manager that you are using:

- For CipherTrust Manager, launch the **CTE** application and create a Profile with the appropriate Quality of Service configuration parameters. Then make sure that all clients in the DFSR configuration use that profile.
 - For the DSM, you need to set the CPU cap on the **GuardPoints** tab for each host in the DFSR configuration.
6. Create the required CTE-LDT GuardPoints using the Live Data Transformation policy you created.

You need to create the same set of GuardPoints, using the same Live Data Transformation policies, on each server in the configuration. For example, let's say you set up the following GuardPoints for the first server:

Guard Path	CTE-LDT Policy Name
D:\data	LDT-Policy-Main
D:\data\DfsrPrivate	LDT-Policy-Main
F:\	LDT-Policy-Main
F:\DfsrPrivate	LDT-Policy-Main
G:\HR Files	LDT-Policy-HR
G:\HR Files\DfsrPrivate	LDT-Policy-HR

You must then set up the same six GuardPoints using the same two CTE-LDT policies on each server in the configuration.

Chapter 8: Secure Start

This chapter describes encrypting an Microsoft Active Directory (AD) with the Secure Start feature. It contains the following topics:

Secure Start Overview	89
Prerequisites	89
Encrypt by Moving the AD Service into a Guarded Directory	90
Encrypt Data in Place with Offline Transformation	91
Encrypt with an LDT Transformation Policy	92
Configure the Time Out Failure	92
Recover a Server After it Loses Connection to the Key Manager	93
Other Use Cases	93
Best Practices for Encrypting and Protecting the AD Service	94

Secure Start Overview

Secure Start offers data protection for applications which start earlier in the boot sequence than VMD (Vormetric Daemon). For example, the Microsoft Active Directory (AD) system service starts very early in the boot sequence. To determine if another application qualifies, contact Thales technical support.

Notes

- Secure Start is included with CTE. You do not have to purchase it separately.
- Secure Start is supported on Windows Server 2008 R2 and later versions.

There are three methods for encrypting the AD directory:

- ["Encrypt by Moving the AD Service into a Guarded Directory" on the next page](#)
- ["Encrypt Data in Place with Offline Transformation" on page 91](#)
- ["Encrypt with an LDT Transformation Policy" on page 92](#)

Prerequisites

Prior to using Secure Start to guard your AD database:

1. Backup your AD database:
 - a. Navigate to **Administrative Tools**.
 - b. Click **Windows Server Backup**.
 - c. Click **Action > Backup Once**.
 - d. Follow the instructions in the Backup Wizard to create a backup of the server in a local drive.

Note: When the backup operation completes, it saves the server backup in `<backup drive>:\WindowsImageBackup\<BackupComputerName>`.

2. Perform a system state backup.
3. Obtain the Microsoft DSRM (Data Services Restore Mode) password.
4. Ensure that your AD database is not in `c:\windows\NTDS`.



WARNING

Do not put your AD database in `c:\Windows` or `c:\Program files`. Secure Start cannot encrypt or decrypt any files in those folders.

Encrypt by Moving the AD Service into a Guarded Directory

You can move the AD service into a directory protected by a standard or LDT production policy. This method does not require the initial data transformation step. When you move the AD service into this directory, CTE immediately encrypts the data with either policy.

Note

This step occurs when the system is in DSRM mode, so users have no access to the AD service.

Create the AD GuardPath directory

Create the directory in which the AD service will reside.

1. Log in to the Active Directory Server in DSRM mode using the DSRM password. User ID is Administrator.
2. Create a folder to which you will move the AD database.

Apply Secure Start GuardPoints to a Directory with the DSM

Access to a Secure Start GuardPoint is only permitted during the boot sequence and for a short period of time. Once the VMD is up and running, it performs the normal agent initialization and communicates with the DSM to access files within a GuardPoint location.

To apply Secure Start GuardPoints in **DSM**:

1. In the DSM, click **Hosts > Hosts > <hostName>**
2. In the General host information section, select the option: **Secure Start GuardPoint**.
3. Click **GuardPoints**.
4. Select the directory and click **Guard**.
5. In the Policy field, select an **LDT** or **Standard Production** policy.
6. Set Type to **Directory (Auto Guard)**.
7. Click **Browse** and navigate to the folder that you just created for the AD database.
8. Select the option: **Secure Start**.
9. Click **OK**.
10. Select the GuardPoint and click **Secure Start On**.

Apply Secure Start GuardPoints to a Directory with CipherTrust Manager

To apply Secure Start GuardPoints in **CM**:

1. In the CipherTrust Manager Applications Page, click **CTE > Clients > <clientName>**.
2. Click **Create GuardPoint**.
3. In the Policy field, select a policy.

4. Set Type to **Auto Directory**.
5. Click **Browse**, navigate to, and select, the folder that you just created for the AD database.
6. Select the option: **Secure Start**.
7. Click **Create**.
8. Click **No** to the question, "Would you like to use these GuardPoint settings on another GuardPoint with a different path?" because you are only guarding the AD database.

Verify the Secure Start GuardPoint with CLI

After the policy is pushed to the Active Directory Server, verify the GuardPoints.

To verify the GuardPoints, type:

```
> voradmin ss verify <GuardPoint_path>
Successfully completed the command verify
Success from kernel -Successfully verified the secure start GP
```

Move the AD Database into the Secure Start GuardPoint

Move your AD database from the default location (c:\windows\NTDS) to this newly created protected folder.

To move the AD database:

1. In DSRM mode, login using the DSRM password. User ID is Administrator.
2. Start NTDSUTIL utility, type:

```
> activate instance ntds
```
3. Type:

```
> files
```
4. Type:

```
> move db to \<GuardPoint>
```
5. Type:

```
> move logs to \<GuardPoint>
```
6. Exit NTDSUTIL utility.
7. Reboot the system into normal mode. The Active Directory Services automatically starts after rebooting.

Note

This step occurs when the system is in DSRM mode, so users have no access to the AD service.

Encrypt Data in Place with Offline Transformation

Encrypting the AD database with a standard (production), or offline policy is very similar to encrypting other data with a standard (production), or offline policy.

The advantage to encrypting data in place is that it saves space. When you copy/move a directory into a guarded directory, you will need twice as much space to store the data because you leave a copy of the data in the original folder, as a precaution, until the original directory has been successfully moved and encrypted. Once the data is transformed, then you can delete the directory that contains the decrypted/clear data.

Using this method, you perform an Initial Data Transformation using the `dataxform` command line utility. During this transformation, access to the GuardPoint data is blocked. After initial transformation, you remove the initial policy, and then apply a production policy, so users can access the data.

Notes

- This step occurs when the system is in DSRM mode, so users have no access to the AD service.
- If your AD service is installed in the default directory, `C:\Windows\NTDS`, you must move it to another directory before you can encrypt it. See ["Encrypt by Moving the AD Service into a Guarded Directory" on page 90](#) for more information.

To encrypt the data:

1. In DSRM mode, login using the DSRM password. User ID is Administrator.
2. Create and apply a `dataxform` policy to the GuardPoint directory.
3. Run the `dataxform` command.
4. Remove the `dataxform` policy on the GuardPoint and replace it with a production policy.
5. Reboot out of DSRM mode.

Encrypt with an LDT Transformation Policy

Encrypting the AD database with an LDT policy uses the same steps as encrypting with a standard production policy. The only difference is that you select an LDT policy instead of a standard one. See ["Encrypt by Moving the AD Service into a Guarded Directory" on page 90](#) for more information.

Note

If your AD service is installed in the default directory, `C:\Windows\NTDS`, you must move it to another directory before you can encrypt it.

Configure the Time Out Failure

During the initial access to a Secure Start GuardPoint, the CTE agent sets a timer. The default duration is 30 seconds, but you can configure the duration. Minimum duration is one second, maximum duration is 300 seconds.

Data inside the GuardPoint is accessible without DSM connectivity until the timeout is reached. VMD service activates and makes a secure connection to the DSM. After the VMD makes a secure connection, the agent verifies that it is connected to correct DSM. If the VMD fails to connect to the DSM, the timeout is reached, and if AD is installed, the agent shuts down the system for data security purposes.

Note

In DSRM mode, when the timeout occurs, CTE removes the keys from memory. However, CTE does not shut down the system.

In normal mode, CTE shuts down the AD server. For any other application, or if AD is not installed, Secure Start does not shut down the server. However, the data inside the GuardPoint becomes inaccessible until DSM connectivity is restored, or you issue a challenge/response, or password. After the timer has expired, CTE denies any further access to the Secure Start GuardPoint.

1. To configure the timeout duration in seconds, use the `voradmin ss settimeout <timeout>` command. For example:

```
C:\> voradmin ss settimeout 220
Successfully completed the command settimeout
Successfully set the Secure Start timeout value to 220 seconds
```

2. To verify the timeout duration, type:

```
C:\> voradmin ss gettimeout  
Successfully completed the command gettimeout  
Secure Start timeout value is set to 220 Seconds
```

Recover a Server After it Loses Connection to the Key Manager

User must unlock the GuardPoint by entering the Challenge/Response or password to restore the DSM connectivity. Once the GuardPoint is unlocked, you can start the AD services manually.

Note

The challenge response pop up dialog does not display in DSRM mode when the host loses DSM connectivity.

To activate the challenge/response:

1. Navigate to:

```
C:\Program  
Files\Vormetric\DataSecurityExpert\agent\shared\bin
```

2. Double-click `etray.exe` to start it manually.

If the AD server does not connect to the DSM, then the AD system automatically shuts down. The Administrator must enter DSRM mode and restore the DSM connectivity to recover the server.

Prerequisites

Before rebooting your active directory servers, ensure that DSM connectivity is strong. If it is not strong, restore the DSM connectivity.

Note

When trying to fix a DSM connectivity issue, you can log in to DSRM mode. In DSRM mode, there is no requirement to increase the timeout, because in DSRM mode, the AD system does not shut down after timeout expires.

DSRM Mode

The first method for recovering a server relies on manual DSM connection troubleshooting:

1. Boot into DSRM mode.
2. Attempt to resolve why the server is not connecting to the DSM.
3. Fix that DSM connectivity issue.
4. Reboot into normal mode.

Other Use Cases

Using Secure Start GuardPoints, you can also secure an SQL Server on Microsoft Azure in certain scenarios. SQL system services in Azure also boot earlier in the boot sequence than the VMD (Vormetric Daemon) agent service.

Note

To determine if another application qualifies, contact Thales technical support.

Boot a Windows Server in Azure

To move and guard the AD database, you must boot the AD server into DSRM mode.

To boot a Windows Server 2012/2016 Domain Controller into DSRM remotely in Azure:

Note

The Windows Server 2012/2016 domain controller must be running and accessible through Windows Remote Desktop.

1. Establish a Remote Desktop session on the domain controller.
2. Open an command prompt as Administrator and type:
> `bcdedit /set safeboot dsrepair`
3. Reboot the domain controller. The Remote Desktop session disconnects.
4. Wait a few minutes, then establish a new Remote Desktop session. The domain controller will be running in DSRM.
5. To reboot into normal mode, open an command prompt as Administrator and type:
> `bcdedit /deletevalue safeboot`
6. Reboot the domain controller.

Best Practices for Encrypting and Protecting the AD Service

Thales recommends the following best practices when using Secure Start with an AD service.

Access Control with Secure Start

User can setup a restricted access control policy with encryption to prevent the unauthorized access of AD database files. The restricted policy with Secure Start:

- Prevents a rogue user from logging into the system, and moving or copying the AD database files to another directory and tampering with it.
- Denies permissions, after you setup and guard files, so that no one can move a file from the guarded directory. Plus it restricts any other unwanted/unnecessary process or users from tampering with AD files.
- Provides permission for an authorized user who needs access to AD services and files.

Creating a Minimal Policy Required for AD with Access Control

When creating a normal, strict policy for access control, you must allow access to the following processes and directories for Active Directory.

Processes

```
secfsd.exe (C:\Program  
Files\Vormetric\DataSecurityExpert\agent\secfs\ sec\bin\  
lsass.exe (C:\Windows\System32\  
vds.exe (C:\Windows\System32\  
vssvc.exe (C:\Windows\System32\  
wbengine.exe (C:\Windows\System32\  
ntoskrnl.exe (C:\Windows\System32\)
```

Users

NT AUTHORITY\SYSTEM

To create a minimal policy:

1. Create a User Set named **AD_Minimum_User_Set** with the following parameters:

ID	uname	osDomains
1	SYSTEM	NT AUTHORITY

2. Create a Process Set named: **AD_Process_Set** with the following parameters:

ID	Directory	Base Name
1	C:\Program Files\Vormetric\DataSecurityExpert\agent\secfs\sec\bin	secfsd.exe
3	c:\Windows\System32\	ntoskrnl.exe
4	c:\Windows\System32\	vds.exe
5	c:\Windows\System32\	vssvc.exe
6	c:\Windows\System32\	wbengine.exe
7	c:\Windows\System32\	lsass.exe

3. Create a Security rule set with the following parameters:

Order	User	Process	Action	Effect	Browsing
1	AD_Minimum_User_Set	AD_Process_Set	all_ops	Audit, Permit, Apply key	Yes
2				Audit, Deny	Yes

Creating a Restricted Policy in DSRM Mode

Create the following policy for the initial transformation of an AD database in DSRM mode. The policy allows access to the local administrator.

In DSRM mode, you use the `NTDSUTIL` utility to perform maintenance for an Active Directory.

To create a restricted policy:

1. Create a User Set named **AD_Minimum_User_Set** with the following parameters:

ID	uname	osDomains
1	SYSTEM	NT AUTHORITY
2	Administrator	localhost

2. Create a Process Set named: **AD_Process_Set** with the following parameters:

ID	Directory	Base Name
1	C:\Program Files\Vormetric\DataSecurityExpert\agent\secfs\sec\bin	secfsd.exe
2	c:\Windows\System32\	ntdsutil.exe
3	c:\Windows\System32\	ntoskrnl.exe
4	c:\Windows\System32\	vds.exe
5	c:\Windows\System32\	vssvc.exe
6	c:\Windows\System32\	wbengine.exe
7	c:\Windows\System32\	lsass.exe

3. Create a Security rule with with the following parameters:

Order	User	Process	Action	Effect	Browsing
1	AD_Minimum_User_Set	AD_Process_Set	all_ops	Audit, Permit, Apply key	Yes
2				Audit, Deny	Yes

Guard Directories

The best practice for guarding a directory with a Secure Start GuardPoint is to:

1. Create a directory.
2. Guard that directory with a standard production or LDT policy. Follow the steps in ["Apply Secure Start GuardPoints to a Directory with the DSM" on page 90](#).
3. Move the AD service into that directory.

Perform Subsequent System State Backups

After you move an AD service into a guarded directory, or out of a guarded directory:

1. Perform another system state backup.
2. Save this subsequent backup to a different location.

Chapter 9: Exchange DAG

This chapter describes encrypting email databases using Microsoft Exchange database availability group (DAG). It contains the following topics:

Exchange DAG Overview	97
Requirements for Exchange DAG Encryption	98
CTE Policies for Exchange DAG	99
Encrypting with CTE-LDT in an Exchange DAG Environment	105
Encrypting with a Standard CTE Policy in the Exchange DAG Environment	108
Decrypting with CTE-LDT in an Exchange DAG Environment	110

Exchange DAG Overview

A DAG is a high-availability (HA) and data-recovery feature of the Microsoft Exchange Server. A DAG, which can consist of up to 16 Exchange mailbox servers, automates recovery at the database level after a database, server or network failure. You can now use CTE for Windows to encrypt Exchange DAG mailboxes.

You can encrypt the Exchange databases with a standard (offline) policy or an CTE-Live Data Transformation (CTE-LDT) policy. In an offline policy, users cannot access the database during initial data encryption. With a CTE-LDT policy, CTE encrypts the data while users and applications are accessing the files. CTE-LDT is used for Initial data transformation as well as transparent encryption and decryption.

Note

For more information about CTE-LDT and standard data transformation, see *CTE-Live Data Transformation with CipherTrust Manager*, *CTE-Live Data Transformation with Data Security Manager*, or the *CTE Data Transformation Guide*. All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)

Supported Use Cases for CTE in an Exchange DAG Environment

CTE has been tested by Thales in the following scenarios:

- Initial data transformation of Exchange databases using either CTE-Live Data Transformation or standard data transformation.
- Transparent encryption or decryption of the Exchange database on DAG nodes.
- Key rotation using a CTE-LDT policy.

Thales also tested the following Exchange DAG operations during the above scenarios:

- Failover/Failback of databases from one node to another node and making both databases active on each node.
- Adding new Databases to the existing nodes.

Unsupported Use Cases

The following scenarios are not supported:

- Using different encryption keys on Exchange DAG nodes; both nodes must use the same encryption key
- Adding a new node to the Exchange DAG Environment. CTE only supports two Exchange DAG nodes.
- The encryption of Exchange Binaries.
- Using nodes in a different subnet, data center, or site. (Thales is not testing this scenario, but we do not believe it will cause any issues.)

Requirements for Exchange DAG Encryption

The following things are required for CTE encryption in an Exchange DAG environment:

- Windows Exchange Server 2016 Cumulative Patch 5.
- Windows Server 2016 for the Exchange Server nodes.
- A Windows 2016 Server as a file share witness.
- Two nodes in the Exchange DAG configuration. CTE does not support more than two Exchange DAG nodes.
- The CTE Agent must be installed on both Exchange DAG nodes. In addition, both CTE Agents must be registered with the same key manager. For details, see [Chapter 2: "Getting Started with CTE for Windows" on page 14](#).
- If you want to use CTE-Live Data Transformation (CTE-LDT), make sure that the license for this feature is installed and activated in your key manager. CTE-LDT is a separately licensed feature of CTE.
- The same CTE Policy and encryption key must be used on both nodes.
 - If you are going to use CTE-LDT, you must use a *versioned* CBC or CBC_CS1 key. For details, see ["Creating a Policy for CTE-LDT Encryption with CipherTrust Manager" on the facing page](#) or ["Creating a Policy for CTE-LDT Encryption with the DSM" on page 103](#).
 - If you are going to use Standard encryption, you must create both an initial encryption policy and a production policy. For details, see ["Creating Policies for Standard Encryption with CipherTrust Manager" on page 100](#) or ["Creating Policies for Standard Encryption with the DSM" on page 103](#).
- Secure Start must be enabled on all GuardPoints.
- All users must be offline when the initial GuardPoint is applied, even with a CTE-Live Data Transformation policy.

Note: Alternatively, you can choose to make all of the databases active on one node and perform data transformation on the other node. The procedures later in this chapter use this method.

- Thales recommends that you disable all antivirus software as suggested by Microsoft.
[https://technet.microsoft.com/en-us/library/bb332342\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/bb332342(v=exchg.160).aspx)
- Windows Defender must be disabled.
<https://www.wintips.org/how-to-disable-or-remove-windows-defender-antivirus-in-server-2016/>
- You can only guard one host at a time. Do not use a Host Group to assign GuardPoints.
- The CTE Agent must be able to communicate with the key manager.

CTE Policies for Exchange DAG

The CTE policies you need depend on the type of encryption you will be using.

- When you use CTE-LDT encryption, you only need to create one Live Data Transformation policy. This policy will be used for both the initial data encryption and guarding the data in production. CTE-LDT requires a versioned CBC or CBC_CS1 key in order to perform automatic key rotation.
- When you use standard encryption, you need to create two policies:
 - The *initial encryption* policy specifies the current encryption key (if any) and the encryption key you want CTE to use when it encrypts the data. This policy also denies access to any other process trying to access the GuardPoint.
You apply the initial encryption policy when you first create the GuardPoint, and you leave it in place until all of the data has been encrypted. After that, you remove this policy from the GuardPoint.
 - The *production* policy specifies the same encryption key as the initial encryption policy along with any security rules you want to use to protect your data in production. After the initial encryption has completed, you apply the production policy to the GuardPoint and allow users and applications to access the now-protected data.

Note

There are no special CTE policy requirements for Exchange DAG with either CTE-LDT or Standard encryption. Therefore, you can use the same policies in an Exchange DAG environment that you use for any other CTE-protected directory.

The only special requirement for Exchange DAG is the guard path you specify when you create the GuardPoint. You must guard the Mailbox directory only. Do not guard above or below the Mailbox directory. For details, see ["Encrypting with CTE-LDT in an Exchange DAG Environment" on page 105](#) or ["Encrypting with a Standard CTE Policy in the Exchange DAG Environment" on page 108](#).

How you create these policies depends on the key manager that you are using. For details, see one of the following:

- ["Creating a Policy for CTE-LDT Encryption with CipherTrust Manager" below](#)
- ["Creating Policies for Standard Encryption with CipherTrust Manager" on the next page](#)
- ["Creating a Policy for CTE-LDT Encryption with the DSM" on page 103](#)
- ["Creating Policies for Standard Encryption with the DSM" on page 103](#)

Creating a Policy for CTE-LDT Encryption with CipherTrust Manager

When you use CTE-LDT encryption, you only need to create one policy. This policy will be used for both the initial data encryption and guarding the data in production. CTE-LDT requires a versioned CBC or CBC_CS1 key in order to perform automatic key rotation. For details, see the *CTE-Live Data Transformation with CipherTrust Manager* guide for the version of CTE that you are using. All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)

Note

The following procedure describes how to create this policy with CipherTrust Manager. If you are using the DSM, see ["Creating a Policy for CTE-LDT Encryption with the DSM" on page 103](#).

1. Log into CipherTrust Manager and launch the **CTE** application.
2. In the left-hand menu bar, click **Policies**.
3. Click **Create Policy**.

4. For **Name**, make sure you use a name that clearly designates this as a CTE-LDT policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
5. For **Policy Type**, select **Live Data Transformation**.
6. Click **Next** to go to the Security Rules page. CipherTrust Manager should have automatically added a security rule for **Action**: `key_op`, **Effect**: `permit, applykey`. If this security rule is not there, click **Back** and make sure you have selected **Live Data Transformation** in the **Policy Type** field.
7. Enter any other security rules you want to use based on your production environment requirements. You can add as many security rules as you need to define who should have access to the protected data.
For more information about the type of rules you may want to use, or ways to exclude some data from encryption, see the *CTE-Live Data Transformation with CipherTrust Manager* guide for the version of CTE that you are using. All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)
8. When you are done specifying your security rules, click **Next** to go to the Key Rules page.
9. Click **Create Key Rule** and enter the following information:
 - In the **Current Key Name** field, click **Select** to specify the current encryption key used for the data. If the data is unencrypted, specify `clear_key` as the encryption key.
 - In the **Transformation Key Name** field, click **Select** to specify the versioned encryption key you want to use to encrypt the data. When you are done, click **Add**.

Tip: You can also create a new key at this point if desired. For details on creating an encryption key, see your CipherTrust Manager documentation.

For example:

Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule	
	clear_key	VersionedKey-AES256	No	...

10. Click **Next** to go to the Confirmation page.
11. Verify your selections and click **Save** to save the policy.

Creating Policies for Standard Encryption with CipherTrust Manager

When you use standard encryption, you need to create two policies:

- The *initial encryption* policy specifies the current encryption key (if any) and the encryption key you want CTE to use when it encrypts the data. This policy also denies access to any other process trying to access the GuardPoint.
You apply the initial encryption policy when you first create the GuardPoint, and you leave it in place until all of the data has been encrypted. After that, you remove this policy from the GuardPoint.
- The *production* policy specifies the same encryption key as the initial encryption policy along with any security rules you want to use to protect your data. After the initial encryption has completed, you apply the production policy to the GuardPoint and allow users and applications to access the now-protected data.

Note

The following procedures describe how to create these policies with CipherTrust Manager. If you are using the DSM, see "[Creating Policies for Standard Encryption with the DSM](#)" on page 103.

Creating the Initial Encryption Policy

1. Log into CipherTrust Manager and launch the **CTE** application.
2. In the left-hand menu bar, click **Policies**.
3. Click **Create Policy**.
4. For **Name**, make sure you use a name that clearly designates this as an initial-encryption policy and not a production policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
5. For **Policy Type**, select **Standard**.
6. Enable the **Data Transformation** check box.
7. Click **Next** to go to the Security Rules page. CipherTrust Manager should have automatically added a security rule for **Action:** `key_op`, **Effect:** `permit,applykey`. If this security rule is not there, click **Back** and make sure you have enabled the **Data Transformation** check box.
8. Click **Create Security Rule** and do the following:
 - a. In the **Action** field, select `all_ops`.
 - b. In the **Effect** field, select `deny`.
 - c. Click **Add** to return to the Security Rules page.

You should now have two security rules, as shown:

Resource Set	User Set	Process Set	Action	Effect	Browsing	
▶			key_op	permit,applykey	Yes	...
▶			all_ops	deny	Yes	...

9. Click **Next** to go to the Key Rules page.
10. Click **Create Key Rule**.
11. In **Current Key Name**, click **Select** to specify the current encryption key used for the data. If the data is unencrypted, specify `clear_key` as the encryption key. When you are done, click **Add**. For example:

Resource Set	Current Key Name	
	clear_key	...

Tip: You can also create a new key at this point if desired. For details on creating an encryption key, see your CipherTrust Manager documentation.

12. Click **Next** to go to the Data Transformation page.
13. Click **Create Data Transformation Rule**.

14. In the **Transformation Key Name** field select the encryption key you want to use to encrypt the data. This key must match the one specified in the production policy you intend to apply to the GuardPoint after the data has been encrypted. For example, if you want to encrypt the data with the key CS1_AES256, you would specify the following transformation rule:

Resource Set	Transformation Key Name
	CS1-AES256 ...

15. Click **Next** to go to the Confirmation page.
16. Verify your selections and click **Save** to save the policy.

Creating the Production Policy

1. Launch the **CTE** application.
2. In the left-hand menu bar, click **Policies**.
3. Click **Create Policy**.
4. For **Name**, make sure you use a name that clearly designates this as a production policy and not an initial encryption policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
5. For **Policy Type**, select **Standard**.
6. Click **Next** to go to the Security Rules page. Enter the security rules you want to use based on your production environment requirements. You can add as many security rules as you need to define who should have access to the protected data.
7. When you are done, click **Next** to go to the Key Rules page.
8. Click **Create Key Rule**.
9. In **Key Name** field, click **Select** to specify the encryption key used to transform the data in the initial encryption policy. When you are done, click **Add**. For example:

Resource Set	Key Name
	CS1-AES256 ...

10. Click **Next** to go to the Data Transformation page.
11. Click **Create Data Transformation Rule**.
12. In the **Transformation Key Name** field select the encryption key you want to use to encrypt the data. This key must match the one specified in the production policy you intend to apply to the GuardPoint after the data has been encrypted. For example, if you want to encrypt the data with the key CS1_AES256, you would specify the following transformation rule:

Resource Set	Transformation Key Name
	CS1-AES256 ...

13. Click **Next** to go to the Confirmation page.
14. Verify your selections and click **Save** to save the policy.

Creating a Policy for CTE-LDT Encryption with the DSM

When you use CTE-LDT encryption, you only need to create one policy. This policy will be used for both the initial data encryption and guarding the data in production. CTE-LDT requires a versioned CBC or CBC_CS1 key in order to perform automatic key rotation. For details, see the *CTE-Live Data Transformation with Data Security Manager* guide for the version of CTE that you are using. All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)

Note

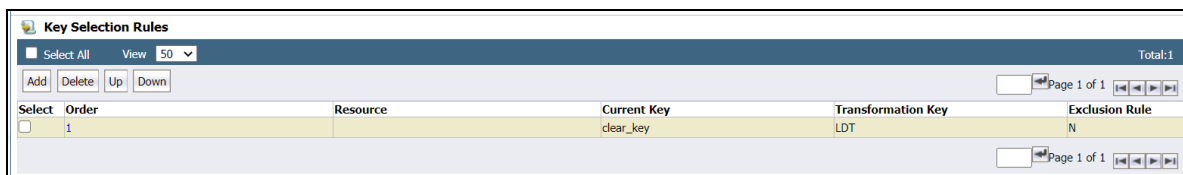
The following procedure describes how to create this policy with the DSM. If you are using CipherTrust Manager, see "[Creating a Policy for CTE-LDT Encryption with CipherTrust Manager](#)" on page 99.

1. Log into the DSM Management Console and switch to the domain containing the host you want to protect.
2. In the top menu bar, click **Policies**.
3. Above the policy table, click **Add**.
4. For **Policy Type**, select **Live Data Transformation**.
5. For **Name**, make sure you use a name that clearly designates this as a CTE-LDT policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
6. In the Security Rules section, the DSM automatically adds a security rule for **Action:**key_op, **Effect:** Apply Key, Permit. Enter any other security rules you want to use based on your production environment requirements. You can add as many security rules as you need to define who should have access to the protected data.

For more information about the type of rules you may want to use, or ways to exclude some data from encryption, see the *CTE-Live Data Transformation with Data Security Manager* guide for the version of CTE that you are using. All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)

7. In the Key Selection Rules area, click **Add** and enter the following information:
 - In the **Current Key** field, click **Select** to specify the current encryption key used for the data. If the data is unencrypted, specify `clear_key` as the encryption key.
 - In the **Transformation Key** field, click **Select** to specify the versioned encryption key you want to use to encrypt the data. When you are done, click **Ok**.

For example:



Select	Order	Resource	Current Key	Transformation Key	Exclusion Rule
<input type="checkbox"/>	1		clear_key	LDT	N

8. Click **OK** to save the policy.

Creating Policies for Standard Encryption with the DSM

When you use standard encryption, you need to create two policies:

- The *initial encryption* policy specifies the current encryption key (if any) and the encryption key you want CTE to use when it encrypts the data. This policy also denies access to any other process trying to access the GuardPoint.

You apply the initial encryption policy when you first create the GuardPoint, and you leave it in place until all of the data has been encrypted. After that, you remove this policy from the GuardPoint.

- The *production* policy specifies the same encryption key as the initial encryption policy along with any security rules you want to use to protect your data. After the initial encryption has completed, you apply the production policy to the GuardPoint and allow users and applications to access the now-protected data.

Note

The following procedures describe how to create these policies with the DSM. If you are using CipherTrust Manager, see "[Creating Policies for Standard Encryption with CipherTrust Manager](#)" on page 100.

Creating the Initial Encryption Policy

- Log into the DSM Management Console and switch to the domain containing the host you want to protect.
- In the top menu bar, click **Policies**.
- Above the policy table, click **Add**.
- For **Policy Type**, select **Standard**.
- For **Name**, make sure you use a name that clearly designates this as an initial-encryption policy and not a production policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
- Add a security rule with:
 - Action:** `key_op`
 - Effect:** `Apply Key, Permit`
- Add a second security rule with:
 - Action:** `all_ops`
 - Effect:** `Audit, Deny`

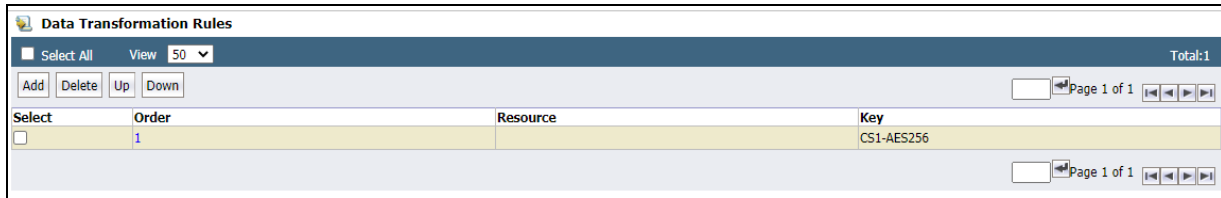
For example:

Select	Order	Resource	User	Process	Action	Effect	When	Browsing
<input type="checkbox"/>	1				key_op	Apply Key, Permit		Yes
<input type="checkbox"/>	2				all_ops	Audit, Deny		Yes

- Add a Key Rule that specifies the current encryption key used for the data. If the data is unencrypted, specify `clear_key` as the encryption key. For example:

Select	Order	Resource	Key
<input type="checkbox"/>	1		clear_key

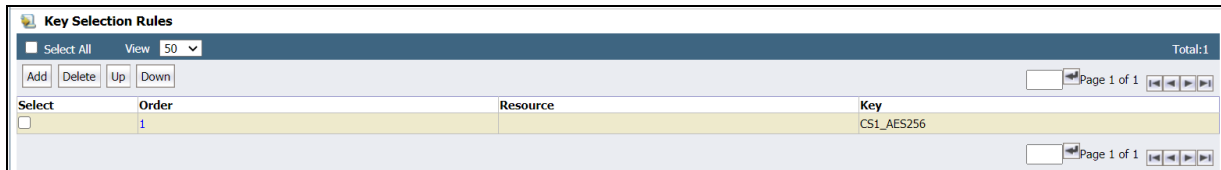
9. Add a Data Transformation Rule that specifies the encryption key you want to use to encrypt the data. This key must match the one specified in the production policy you intend to apply to the GuardPoint after the data has been encrypted. For example, if you want to encrypt the data with the key CS1_AES256, you would specify the following transformation rule:



10. Click **OK** to save the policy.

Creating the Production Encryption Policy

1. Log into the DSM Management Console and switch to the domain containing the host you want to protect.
2. In the top menu bar, click **Policies**.
3. Above the policy table, click **Add**.
4. For **Policy Type**, select **Standard**.
5. For **Name**, make sure you use a name that clearly designates this as a production policy and not a initial encryption policy. You will need to be able to find this policy name from the list of all available policies when you create the GuardPoint.
6. In the Security Rules area, enter the security rules you want to use based on your production environment requirements. You can add as many security rules as you need to define who should have access to the protected data.
7. In the Key Rules area, add a Key Rule that specifies the encryption key specified in the Data Transformation Rule in the initial encryption policy. For example:



8. Click **OK** to save the policy.

Encrypting with CTE-LDT in an Exchange DAG Environment

Prerequisites

Before you can start the CTE-LDT data encryption process, you need to:

- Create or identify the CTE policy you want to use for data encryption. CTE-LDT uses a single Live Data Transformation policy for both initial encryption and subsequent rekeys, so the policy you use should have all the access control rules you want to use for your data when it is in production. For details, see ["CTE Policies for Exchange DAG" on page 99](#).
- Set your Quality of Service (QoS) settings. QoS enables administrators to manage and control CTE-LDT impact to application workloads by monitoring and controlling the use of host system resources, such as memory or I/O utilization, during data transformation.

For details about using CTE-LDT, see *CTE-Live Data Transformation with Data Security Manager* or *CTE-Live Data Transformation with CipherTrust Manager* for the version of CTE that you are using. All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)

Procedure

1. In the **Exchange Admin Center**, make Exchange node 1 the primary node.
Make node 1 the active node and move all of the databases to that node.
2. Make all of the databases active on node 1.
3. Suspend all databases on node 2. Wait for 2-3 minutes for the database to finish with replication so the database will be suspended.



WARNING

Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases. All Exchange Services must be stopped, all databases must be suspended, and all data replication between the nodes must be stopped. Any file access on the node during the encryption process could cause data corruption.

4. When you are certain that all Exchange DAG services have been suspended on node 2, create the GuardPoints you want to use on node 2 with the appropriate Live Data Transformation policy. When you create the GuardPoints:
 - Make sure you are guarding each host individually. Do *not* assign the GuardPoints using a Host or Client Group because you only want these GuardPoints to exist on node 2 at this point.
 - **Important:** When you specify the guard path, only guard the Mailbox Database. Do *not* guard at a higher or lower directory. For example:
 - **Correct:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\
 - **Incorrect:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\Inbox\ — This is *not* correct because it's below the mailbox database directory.
 - Make sure that **Secure Start** is on for the GuardPoints.

The following example shows two correctly-specified GuardPoints in CipherTrust Manager:


Status	Policy	Protected Path	Type	Client Group	Rekey Status	Enabled
Active	Dataform...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 2035273064	directory_auto	-	N/A	Yes
Active	Dataform...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171	directory_auto	-	N/A	Yes

The following example shows the same two GuardPoints in the DSM:

Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Secure Start
<input type="checkbox"/>	Dataform_clear_2_AES256_Normal		C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\		Directory (Auto Guard)	Guard883	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Dataform_clear_2_AES256_Normal		C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 2035273064\		Directory (Auto Guard)	Guard883	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Live data transformation on node 2 begins as soon as the GuardPoints become active on node 2.

5. Wait until CTE-LDT has finished transforming the data in all GuardPoints on node 2.
6. In the **Exchange Admin Center**, go to the Exchange Database tab and **Resume** all Passive database copy on node 2.
7. Wait for the server to move to the healthy state. If it does not, wait for some more time for the Content Index state to change to Healthy.

 **WARNING**
 It may take a few minutes for the Exchange Service to resync. Monitor the Exchange logs on the system and make sure that replication is working. Make sure that database replication finishes and databases are in a healthy state before proceeding.

8. In the **Exchange Admin Center**, move all of the databases from node 1 to node 2. Now the databases on node 1 are mounted as passive. All databases on node 2 are mounted as active.

9. Create the same GuardPoints on node 1 that you created on node 2. Make sure that all GuardPoints on node 1 are identical to those on node 2.



WARNING

You must guard the same databases with the same Live Data Transformation Policy and the same encryption key on both nodes.

Encrypting with a Standard CTE Policy in the Exchange DAG Environment

Prerequisites

Before you can start the standard (offline) data encryption process, you need to:

- Decide if you will be using the copy/restore method or the `CTEdataxform` utility in order to perform the initial encryption. For details about these methods and their specific benefits and limitations, see the *CTE Data Transformation Guide* for the version of CTE that you are using. All All 7.2 documentation is available at [CTE Docs](#). All 7.3 documentation is available at: [CTE Doc Portal](#)
- Create or identify the encryption key that you want to use for the initial data encryption.
- Create or identify the Standard policies that you want to use for the initial data encryption and for protecting the data in production after it has been initially encrypted. For details, see "[Creating Policies for Standard Encryption with CipherTrust Manager](#)" on page 100 or "[Creating Policies for Standard Encryption with the DSM](#)" on page 103.

Procedure

1. In the **Exchange Admin Center**, make Exchange node 1 the primary node.
This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.
2. Make all of the databases active on Exchange node 1.
3. Go to the Exchange Database tab and suspend all database on node 2.

Make sure that all of the exchange database services in node 2 are down and not accessing the Exchange databases. This process can take several minutes.



WARNING

Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases. All Exchange Services must be stopped, all databases must be suspended, and all data replication between the nodes must be stopped. Any file access on the node during the encryption process could cause data corruption.

4. When you are certain that all Exchange DAG services have been suspended on node 2, create the GuardPoints you want to use on node 2 with the appropriate Standard data transformation policy that you want to use for the initial data encryption. When you create the GuardPoints:
 - Make sure you are guarding each host individually. Do *not* assign the GuardPoints using a Host or Client Group because you only want these GuardPoints to exist on node 2 at this point.
 - **Important:** When you specify the guard path, only guard the Mailbox Database. Do *not* guard at a higher or lower directory. For example:
 - **Correct:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\
 - **Incorrect:** C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\Inbox\ — This is *not* correct because it's below the mailbox database directory.
 - Make sure that **Secure Start** is on for the GuardPoints.

The following example shows two correctly-specified GuardPoints in CipherTrust Manager:

Status	Policy	Protected Path	Type	Client Group	Rekey Status	Enabled
Active	Dataform...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 2035273064	directory_auto	-	N/A	Yes
Active	Dataform...	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171	directory_auto	-	N/A	Yes

The following example shows the same two GuardPoints in the DSM:

Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Secure Start
<input type="checkbox"/>	Dataform_clear_2_AES256_Normal		C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1088388171\		Directory (Auto Guard)	Guard883	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Dataform_clear_2_AES256_Normal		C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 2035273064\		Directory (Auto Guard)	Guard883	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

5. After all GuardPoints on node 2 have been enabled, run the `dataxform` utility for each GuardPoint:


```
dataxform --rekey --print_stat --gp <directory>
```
6. After the data transformation is finished, unguard each mailbox on node 2, then re-guard each mailbox on node 2 with the appropriate Production policy.

Note: Use the same Key/Policy on both nodes.

See the *CTE Data Transformation Guide* guide for more information.

7. In the **Exchange Admin Center**, go to the Exchange Database tab and resume all databases on node 2. After a few minutes, all nodes should become Healthy.



WARNING

It may take a few minutes for the Exchange Service to resync. Monitor the Exchange logs on the system and make sure that replication is working. Make sure that database replication finishes and databases are in a healthy state before proceeding.

8. In the **Exchange Admin Center**, try to move a database from node 1 to node 2. If the data move is successful this means that node 2 is mounted as the active node and node 1 is mounted as the passive node.

9. Create the same GuardPoints on node 1 that you created on node 2. Make sure that all GuardPoints on node 1 are identical to those on node 2.



WARNING

You must guard the same databases with the same Standard Policy and the same encryption key on both nodes.

Decrypting with CTE-LDT in an Exchange DAG Environment

Prerequisites

- Make sure that the LDT state is set to REKEYED before unguarding.
- Make sure that all of the files inside the GuardPoint are at the same version of the key.
 - Run the LDT report to find the version:

```
> voradmin ldt report <GuardPoint path> [<logfile>]
```
 - Run the Key map report to find the version:

```
> voradmin ldt key [report|map] <key_name, version> <GuardPoint path>
```

Procedure

1. Make sure that all of the Exchange services in node 2 are down and not accessing the Exchange databases.

Note: Suspension can take 2-3 Minutes.

2. In the **Exchange Admin Center**, make Exchange node 1 the primary node.
This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.
3. Make all of the databases active on Exchange node 1.
4. Go to the Exchange Database tab and suspend all databases on node 2.
5. Unguard the database folders that you previously guarded on node 2.
6. Delete all of the metadata on all of the database folders on node 2, type:

```
> voradmin ldt attr delete [<file name path> | <guard path>]
```
7. Guard with an LDT policy set for Encryption to Clear on node 2.

Note: You must clone the current version of the encryption key to use as the current key in the new LDT policy and `clear_key` as the transformation key.

8. Go to the Exchange Database tab and resume all databases on node 2.

Note: After a few minutes, the databases should become healthy automatically. If not, wait for the LDT process to decrypt the data. Make sure that all of the data is transformed back to clear and that the LDT state is set to **REKEYED**.

9. Move the database from node 1 to node 2.
10. Repeat this procedure for node 1.

11. After both nodes are rekeyed and transformed from encryption to clear, unguard them:
 - a. In the **Exchange Admin Center**, make Exchange node 1 the primary node.
This means that node 1 is mounted as the active node and node 2 is mounted as the passive node.
 - b. Make all of the databases active on Exchange node 1.
 - c. Go to the Exchange Database tab and suspend all databases on node 2.
 - d. Unguard the database folders that you previously guarded on node 2.



WARNING

Always ensure that you are unguarding a passive node.

- e. Repeat this procedure for Node 1.

Chapter 10: Storage Spaces Direct

This chapter describes how CTE integrates with Windows Storage Spaces Direct (S2D) hyper-converged clusters. It contains the following sections:

S2D Overview	112
Deployment Options	112
Supported Use Cases	113

S2D Overview

S2D uses industry-standard servers with local-attached drives to create high-availability (HA) software-defined storage. S2D is included in Windows Server 2019 Datacenter and Windows Server 2016 Datacenter, both of which are supported by CTE.

S2D extends the stack of usable storage devices to storage devices such as SATA and SAS HDD's, SSD's and NVMe (Non-Volatile Memory Express) disks to create shared disk volumes. S2D supports clusters of a minimum of two nodes, and a maximum of 16 nodes and 400 drives. S2D aggregates the available storage into a Storage Pool.

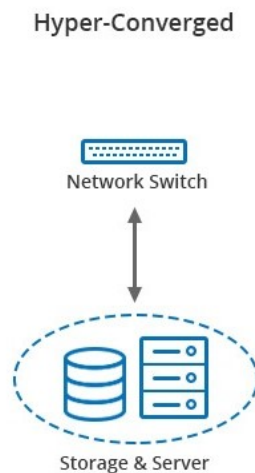
The hyper-converged deployment option runs virtual machines on the servers providing the storage.

A complete description of the S2D product, and instructions on how to set up the S2D environment is available on the Microsoft website at <https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/storage-spaces-direct-overview>

Deployment Options

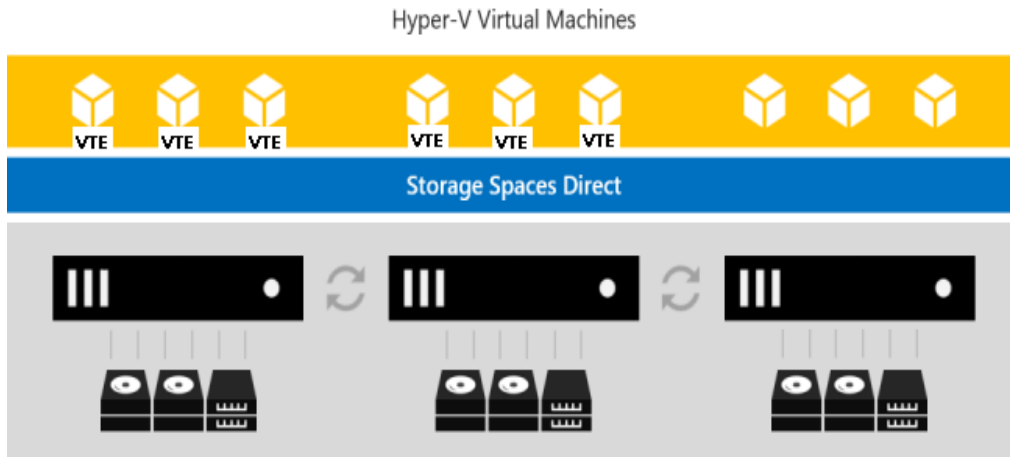
CTE supports S2D in a hyper-converged infrastructure where computing and storage components are in a single cluster as shown in the following figure.

Figure 10-1: Hyper-converged infrastructure



Hyper-converged with S2D and CTE virtual machines run on the servers providing the storage. In the following figure, CTE is installed inside 6 of the VMs to protect the data.

Figure 10-2: High-Level view of S2D



You can use all the capabilities of CTE to protect the data in the VMs in a S2D hyper-converged deployment. These capabilities are described in "[Supported Use Cases](#)" below.

Supported Use Cases

Thales tested only Hyper-converged deployments in the following scenarios.

- Initial Data Transformation of data using:
 - Live Data Transformation
 - Offline Data Transformation
- Transparent Encryption/Decryption of structure and unstructured data
- Key rotation using a Live Data Transformation policy

Chapter 11: Using CTE with Quantum StorNext

This chapter describes how to configure CTE and Quantum StorNext devices to interoperate to allow CTE policies to apply to storage managed by Quantum StorNext.

This section contains the following topics:

Overview of using CTE with Quantum StorNext	114
CTE and Quantum StorNext Compatibility	114
Setting up CTE and Quantum StorNext Integration	116

Overview of using CTE with Quantum StorNext

Quantum StorNext Fibre Channel-connected devices provide shared file access to third party storage for workstation clients and are optimized for simultaneous access to very large files such as video files. The Quantum StorNext file system is known as SNFS or by its older name, CVFS.

You can encrypt and control access to SNFS files with policies by installing CTE Agents on Windows clients that are configured for access to the SNFS file system. Some limitations apply to this integration, such as supported operating systems, supported SNFS features, concurrent read/write access by multiple clients, and GuardPoint settings (see the next section for more information about these limitations).

CTE and Quantum StorNext Compatibility

The following sections list the supported operating systems and CTE settings supported for use with Quantum StorNext file systems. Important unsupported configuration parameters are also listed.

Supported StorNext Server and Client Configurations

The CTE integration with SNFS file systems works only with certain SNFS versions, SNFS storage policies, and client operating systems.

Configuration parameter	Windows
StorNext (SNFS) operating system version	6.x
StorNext metadata controller (MDC) server OS type	Windows MDC supported
StorNext replication policy	Not supported
StorNext deduplication policy	Not supported
StorNext truncation	Supported
StorNext full and partial backup	Supported
StorNext expand file system	Supported
StorNext data migration	Supported
StorNext read-ahead cache	Disable for use with CTE
Client operating systems	Windows Server 2012 R2, Windows Server 2016

Configuration parameter	Windows
StorNext LAN client	DLC
StorNext mount method: locally mounted directory	Supported
StorNext mount method: Windows drive letter	Supported
StorNext mount method: CIFS	Not supported
StorNext mount method: NFS	Not supported

Supported GuardPoint and Key Settings for SNFS File Systems

When configuring CTE GuardPoints and keys for SNFS, keep in the mind the compatibility limitations listed in the following table.

Configuration element	Windows
Offline data transformation	Supported
Live Data Transformation (LDT)	Not supported
Key manager compatibility	See the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> or the <i>Compatibility Matrix for CTE Agent with Data Security Manager</i> for your CTE version
Guard unstructured data	Supported
Guard structured data	Not supported
GuardPoint type: Directory (including entire SNFS volume)	Supported
GuardPoint type: Raw device	Not supported
GuardPoint type: Block device	Not supported
GuardPoint mount option: manual guard	Not applicable
GuardPoint mount option: auto guard	Supported
GuardPoint mount option: automount	Not applicable
AES-CBC key type	Supported
AES-CBC-CS1 key type	Not supported

Supported Concurrent Access Read/Write Scenarios

If you want to allow access by multiple clients (users) to CTE-protected SNFS files under the same GuardPoint, just read-only access is supported. StorNext file locking is not implemented in CTE, so there is currently no way to prevent concurrent conflicting writes to the same file. As a result, Thales does not support write access to the same GuardPoint from multiple clients.

To enable read access to the same GuardPoint from multiple clients, ensure that all clients are configured to use the same policy and key.

Configuration parameter	Windows
Read/write access from a single LAN client to a GuardPoint	Supported
Read/write access from two or more LAN clients to the same GuardPoint	Not supported
Read-only access from one, two, or more LAN clients to the same GuardPoint	Supported

Setting up CTE and Quantum StorNext Integration

For the most part, CTE integration with Quantum StorNext is the same as for any standard file system. The next section provides an overview of the steps involved in making CTE work with SNFS. Later sections provide more information about the steps that are new or differ significantly from a typical CTE setup.

Integration Task Overview

The table below provides an overview of the steps involved in setting up SNFS and CTE to work together. As noted in the table, some of these tasks are described in the documentation for your selected key manager. Some of these steps may need to be performed by other staff members at your organization if you have divided the security administration duties as recommended by Thales and you don't have access to the key manager.

Task	Key configuration notes	For more information
Install and configure a Quantum StorNext MDC server for use with CTE	Disable the StorNext read-ahead cache. Only certain StorNext policies, features, and mount types are supported. See "Supported StorNext Server and Client Configurations" on page 114 .	See "Installing and Configuring a Quantum StorNext MDC Server for Use with CTE" on the next page .
Install and configure Quantum StorNext clients for use with CTE	Only certain operating systems are supported. See "Supported StorNext Server and Client Configurations" on page 114 .	See "Installing and configuring Quantum StorNext DLC Clients for Use with CTE" on the next page .
Create a domain for one or more SNFS hosts, or add them to an existing domain	No difference from standard CTE agent configuration.	See "Domain Management" in your key manager documentation.
Add the host to the key manager	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.
Install and register the CTE Agent on the host system	No difference in installation.	See Chapter 2: "Getting Started with CTE for Windows" on page 14
Create encryption keys (optional)	AES-CBC-CS1 keys are not supported on Windows. See the note in "Supported GuardPoint and Key Settings for SNFS File Systems" on the previous page .	See "Managing Keys" in your key manager documentation. For information about AES-CBC-CS1 keys, see Chapter 4: "Enhanced Encryption Mode" on page 50 .
Configure host groups containing one or more StorNext LAN clients (optional)	No difference from standard CTE agent configuration.	See "Configuring Hosts and Host Groups" in your key manager documentation.

Task	Key configuration notes	For more information
Configure policies (including user, process, and resource sets) to control access or enable encryption	No difference from standard CTE agent configuration.	See “Configuring Policies” in your key manager documentation.
Configure one or more GuardPoints	Some GuardPoint settings are not supported. See " Supported GuardPoint and Key Settings for SNFS File Systems " on page 115.	See “Managing GuardPoints” in your key manager documentation

Installing and Configuring a Quantum StorNext MDC Server for Use with CTE

Install and configure a Quantum StorNext metadata controller (MDC) server using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Windows StorNext MDCs. Ensure that you configure the StorNext server to work with the settings supported by CTE as listed in "[Supported StorNext Server and Client Configurations](#)" on page 114. For example, you must disable the StorNext read-ahead cache and only certain StorNext policies, features, and mount types are supported.

Installing and configuring Quantum StorNext DLC Clients for Use with CTE

Install and configure Quantum StorNext DLC clients using the [Quantum StorNext documentation](#) as a guide. The CTE integration works with Windows StorNext DLCs.

Ensure that you configure DLC clients to work with the settings supported by CTE as listed in "[Supported StorNext Server and Client Configurations](#)" on page 114. For example, only certain operating systems are supported.

Note

Just read-only access is supported if multiple StorNext LAN clients will access files in the same GuardPoint. For more information, see "[Supported Concurrent Access Read/Write Scenarios](#)" on page 115.

Choosing a Mounting Method

There are two methods for mounting a StorNext file system on Windows in the StorNext Client Configuration application:

- Map to Drive Letter
- Map to Directory

Both methods are supported in CTE. If you mount the StorNext file system using the Map to Directory method, you must create the directory on the Windows computer before assigning that directory in the Client Configuration application. For example, the default Map to Directory folder is `C:\Mount\snfs1`. If you use that default, you must create `C:\Mount\snfs1` before mounting the StorNext file system in the Client Configuration application.

If you change mounting methods (drive letter to directory or vice versa), you may need to close and reopen Windows Explorer or reboot the computer for the change to take effect.

Installing the CTE Agent on Each StorNext LAN client

Install a CTE Agent on each computer that is set up as a StorNext LAN client and for which you want to set policies. For supported operating systems, see the table in "[Supported StorNext Server and Client Configurations](#)" on page 114.

Use any installation method supported for your operating system. For details, see [Chapter 2: "Getting Started with CTE for Windows"](#) on page 14.

Chapter 12: Upgrading CTE on Windows

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

This chapter contains the following sections:

To Upgrade in Windows Silently	119
Verify the Windows Installation	119
Resolving Problems that Prevent Silent Install	119
CTE Scheduled Upgrade	120
Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades	121

To Upgrade in Windows Silently

If you have already installed CTE on a Windows computer and want to upgrade it silently, use the appropriate command below for the type of installation binary that you are using.

Note

The protected host must be able to connect to the DSM that it is registered to or the upgrade will fail.

Upgrade using self-extracting .exe

```
vee-fs-7.5.0-78-win64.exe /s /v" /qn"
```

Upgrade using MSI

```
msiexec.exe /i vee-fs-7.5.0-78-win64.msi /qn REINSTALLMODE=voums REINSTALL=ALL
```

Before upgrading using MSI, you must rename the installation file to the name of the previously used MSI installation file. See "[Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades](#)" on page 121 for more information.

Note

For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the protected host must be able to connect to the DSM that it is registered to or the upgrade will fail.

Verify the Windows Installation

After running a silent install, verify the installation by checking CTE processes.

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

Resolving Problems that Prevent Silent Install

If you encounter problems using MSI or self-extracting .exe silent install commands, first check the syntax of the command. To further investigate installation issues, you can use Microsoft diagnostics software:

- For desktop versions of Windows: [Microsoft Diagnostics Troubleshooting Wizard](#)
- For server versions of Windows: [Microsoft Automatic Troubleshooting Services \(MATS\)](#)

Refer to the Microsoft documentation on the linked pages for more information. See the *Compatibility Matrix for CTE Agent with Data Security Manager* for a list of versions of Windows that are supported for use with CTE.

CTE Scheduled Upgrade

Scheduled upgrade allows you schedule an upgrade of the CTE agent to occur after the next time the server hosting the agent reboots normally. Scheduled upgrade can minimize CTE service interruptions. Also, scheduled upgrade can reduce coordination issues in organizations where the security roles are separated.

Notes

- Install all Microsoft update patches before scheduling a CTE Agent upgrade. Otherwise, the upgrade will fail.
- The CTE scheduled upgrade feature is compatible with Windows Server 2008 R2 and higher versions.
- Currently, you can only upgrade a VTE for Windows host to CTE version 7.5.0.78 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.
- For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the protected host must be able to connect to the DSM that it is registered to or the upgrade will fail.
- When upgrading from a CTE version that is prior to v7.1, you must **first** upgrade to v7.1 before scheduling an upgrade to subsequent versions from v7.1.

Scheduling a CTE Upgrade on the Command Line

To schedule CTE to upgrade the next time the system reboots, type:

```
> voradmin upgrade schedule <CTE setup executable path>
```

Self-extracting .exe Example

```
> voradmin upgrade schedule C:\7.5.0.78\vee-fs-7.5.0-78-win64.exe
```

MSI Example

```
> voradmin upgrade schedule C:\7.5.0.78\vee-fs-7.5.0-78-win64.msi
```

System Response

```
Creating and installing service to upgrade. CTE agent will be upgraded on next reboot.
```



WARNING

If you have scheduled an upgrade on reboot and the system crashes or is not shutdown gracefully, you must restart the system again to upgrade the agent.

Scheduling a CTE Upgrade Interactively (self-extracting .exe only)

When you open the self-extracting .exe CTE installation binary and a version of CTE is already installed, you have the option of upgrading immediately or initiating a scheduled upgrade. See the procedure below for details. This is an alternative to scheduling an update on the command line using `voradmin` (see ["Scheduling a CTE Upgrade on the Command Line" above](#)).

1. Move the self extracting .exe CTE installation binary to the computer on which you want to initiate the scheduled upgrade.
2. Double-click the self extracting .exe CTE installation binary to run it.
3. Click through the standard initial dialog boxes like the license dialog box.
4. On the **UPGRADE - Install now or Later** dialog box, click **Schedule Upgrade on next reboot** and then click **Next**.
5. Click **Schedule** on the confirmation dialog box.
The next time the computer reboots, the upgrade will occur.

This interactive method of scheduling an update is not available for MSI CTE installation binaries. You must use the `voradmin` command line scheduled upgrade method.

Show Scheduled CTE Upgrades

To display all scheduled CTE agent upgrades, type:

```
> voradmin upgrade show
```

System Response

```
Current version:      6.0.3.12
Target upgrade version: 6.0.3.15
Upgrade on reboot:    Enabled
```

Cancel a Scheduled CTE Upgrade

To cancel/cleanup a scheduled CTE agent upgrade, type:

```
> voradmin upgrade cancel
```

System Response

```
CTE agent upgrade canceled successfully.
```

Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades

When performing an upgrade, Windows Installer Package (MSI) expects the name of the installation binary to be the same as the binary that you used to install CTE. Because Thales includes the software version and build number in the binary file name, you must rename the installation binary to the name of the previously used MSI installation binary before upgrading using MSI. This applies to any MSI CTE upgrade method: typical (interactive), silent upgrade, and scheduled upgrade. If the name does not match the previous binary file name, the upgrade will fail with error code 1316.

For example, let's say that you installed the CTE Agent using the following installation file:

```
vee-fs-7.4.0-win64.msi
```

If you used this binary to install or upgrade CTE, the next time you want to upgrade CTE the installation binary that you download from Thales might have the following file name:

```
vee-fs-7.5.0.78-win64.msi
```

To upgrade successfully using MSI, you would need to rename the new installation binary to the previous file name of `vee-fs-7.4.0-win64.msi` before upgrading.

Finding The Name Used For A Previous MSI Installation or Upgrade

If you want to upgrade CTE using an MSI installation binary but don't know the file name that you used during the previous installation or upgrade, you can look it up by using one of the following methods on the computer where you installed CTE:

MSI File Name Lookup Method 1: PowerShell

Run the following command in PowerShell:

```
PS> (Get-WmiObject Win32_Product | where { $_.Name -match "CipherTrust Encryption Expert  
File System Agent" }).PackageName
```

Rename the new CTE setup installation binary to the file name output from the PowerShell command and proceed with the upgrade.

MSI File Name Lookup Method 2: Windows Registry

Find the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Product\  
905CB36BF7940894995701C86901D14F
```

Rename the new CTE installation binary to the file name in the registry and proceed with the upgrade.

Chapter 13: Uninstalling CTE from Windows

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

This chapter contains the following sections:

Considerations	123
Procedure	123

Considerations

- The CTE Agent must be removed from the Windows host before the host is removed from the key manager with which it is registered.
- Database applications like DB2 and Oracle can lock the user space while they run. If the uninstall fails because a GuardPoint is in use, determine which applications are using the files in the GuardPoint and stop them. Then run the uninstall again.

Procedure

1. Stop any application from accessing files in the GuardPoint.
2. In the key manager with which this host is registered, do the following:
 - Decrypt any data you want to use after uninstall. After the CTE Agent software is removed, access to data is no longer controlled. If data was encrypted, it will remain encrypted. If decrypted or copied out of the GuardPoint, the data is visible as clear text.

This decryption must be done on *every* GuardPoint on the host if you want to access all existing data on the host.
 - Make sure the Agent and System locks have been disabled for the host.
 - Thales recommends that you remove all GuardPoints from the host before you uninstall the CTE Agent.

Do not remove the host from the key manager yet.
3. Log on to the host as with system administrator privileges.
4. Use one of the following methods to uninstall the CTE Agent:
 - Use the standard Windows Add/Remove program utility from the Control Panel to remove the CTE software.
 - If you installed the CTE Agent using the MSI file, you can uninstall it using the command line with the `msiexec.exe /x Installation_executable /qn` command. For example:

```
C:\> msiexec.exe /x vee-fs-7.5.0-78-win64.msi /qn
```
5. Reboot the system when prompted.
6. Remove the host record from the key manager.

Appendix A: Troubleshooting and Best Practices

Windows Systems

CTE will not register with the DSM

- If there is a firewall between the DSM and CTE, configure `vmd.exe` as a firewall exception on DSM for Windows. Otherwise, the DSM is unable to browse CTE.
- If using a Windows XP or Windows 2003 system Firewall, select **Control Panel > Windows Firewall > Exceptions > Add Program...** and browse for `vmd.exe`. The default location is
`C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmd.exe`
- If using a Windows 7 system Firewall, select **Control Panel > System and Security > Windows Firewall > Allowed Programs...** click **Change settings**, click **Allow another program** and browse for `vmd.exe`. The default location is
`C:\Program Files\Vormetric\DataSecurityExpert\agent\vmd\bin\vmd.exe`

CTE with NFSv4: Permission denied error

You may see a permission denied error if you try to access files on an NFSv4 file system that is guarded by CTE.

CTE imposes a restriction on NFSv4 file systems to prevent write-only permissions from being set on individual files. You can work around this restriction by configuring read and write permissions on the same files.

You can also add a policy that allows write permissions.

This restriction applies only in the case of files resident in guarded NFSv4 file systems.

McAfee VirusScan Enterprise + Antispyware Enterprise

You must install McAfee AV software **before** installing CTE agent. If CTE is installed first, McAfee cannot initialize and all attempts to scan fail.

THALES

Contact us

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

> cpl.thalesgroup.com <

