THALES

Windows User Guide

FOR CTE V7.6.0

CTE Agent for Windows Advanced Configuration Guide Release

This document covers the following information:

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 guide uses the following terminology:

Term	Description
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. **Notes** • This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". • For example, the default installation directory is C:\Program Files\Vormetric\DataSecurityExpert\agent. • For example, the default installation directory is /opt/vormetric/DataSecurityExpert/agent/ for Linux and AIX, and C:\Program Files\Vormetric\DataSecurityExpert\agent\ for Windows.
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.
key manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. Thales offers CipherTrust Manager - a key manager for use with CTE.
host / client	In this documentation, host and client are used interchangeably to refer to the physical or virtual machine on which the CTE Agent is installed.
GuardPoint	A device or directory to which a CTE data protection and encryption policy has been applied. CTE will control access to, and monitor changes in, this device and directory, encrypting new or changed information as needed.

CTE Components

The CTE solution consists of two parts:

- The *CTE Agent software* that resides on each protected virtual or physical machine (host). The CTE Agent performs the required data encryption and enforces the access policies sent to it by the *key manager*. The communication between the CTE Agent and the key manager is encrypted and secure.

  After the CTE Agent has encrypted a device on a host, that device is called a GuardPoint. You can use CTE to create GuardPoints on servers on-site, in the cloud, or a hybrid of both.
- A *key manager* that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles. After you install the CTE Agent on a host and register it with a key manager, you can use the key manager to specify which devices on the host that you want to protect, what encryption keys are used to protect those devices, and what access policies are enforced on those devices.

Note

For a list of CTE versions and supported operating systems, see the CTE Compatibility 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 key manager through a web browser. You must have administrator privileges to create policies using 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.

Getting Started with CTE for Windows

This section 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
- Installing CTE with No Key Manager Registration
- Configuring CTE for Windows with CipherTrust Manager
- Multifactor Authentication for CTE GuardPoints
- Choosing a Login Name Type
- Ransomware Protection
- Guarding Data on CIFS Servers and Clients

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.

1. If you want to install the CTE Agent without registering with a key manager, see Installing CTE with No Key Manager Registration. 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 Configuring CTE for Windows with CipherTrust Manager.
2. Create your policies, encryption keys, and GuardPoints using the selected key manager. For details, see Guarding a Device with CipherTrust Manager.

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.

If you want to register the CTE Agent immediately after installing it, see Configuring CTE for Windows with CipherTrust Manager.

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**.

   Note

   - 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 CipherTrust Manager

This section describes how to install and configure CTE on Windows systems that you plan to register with a CipherTrust Manager.

The installation and configuration process consists of three basic steps:

1. Installation Prerequisites

   Gather the information needed for the installation and set up your network.

2. Interactive Installation on Windows

   Install CTE interactively on a protected host and register the protected host with CipherTrust Manager.

   Silent Installation on Windows

   Install CTE silently (non-interactive) on a protected host and register the protected host with CipherTrust Manager.

3. Registration

   Register the protected host with CipherTrust Manager and make sure that CipherTrust Manager and CipherTrust Transparent Encryption can communicate with each other. This can be done as part of the initial installation or at any point after the CTE Agent has been installed.

4. External Certificates

   Use for communication between CTE and CM. Install the external certificate before registering CipherTrust Transparent Encryption with CipherTrust Manager.

5. Validating CipherTrust Manager and CipherTrust Transparent Encryption with a Local CA Certificate

   Ensure that registration by the CTE agent is serviced only by the expected key manager by providing a copy of the CA certificate that will be used to authenticate the TLS communications with the key manager.

6. Setting the CM log for Ransomware Protection

   Configure the logging level for CipherTrust Manager for Ransomware Protection.

Installation Prerequisites

This section lists the installation requirements and options you should consider before installing CTE.

Installation Method Options

Requirements

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.
- **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.

Network Setup Requirements

- The IP addresses, routing configurations, and DNS addresses must allow connectivity of the Windows system on which you plan to install CTE to the CipherTrust Manager. After the Windows system is registered as a client with the CipherTrust Manager, the client must be able to poll the CipherTrust Manager in case there are any changes to the encryption keys, policies, or GuardPoints.
- It must also allow for connectivity of the CipherTrust Manager to all clients where you install CTE as well as communication between different CTE clients that plan to enable LDT over NFS/CIFS.
- If the system is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

The following port information applies to both Windows and Linux systems.

Communication through a Firewall

If a protected client must communicate with CipherTrust Manager through a firewall, see the CipherTrust Manager documentation to determine which of the ports must be opened through the firewall.

Communication with CipherTrust Manager

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

Communication for LDT over CIFS/NFS

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

- 7024
- 7025

Note

When you are registering a CipherTrust Transparent Encryption client with CipherTrust Manager, you can manually include a destination port number, (Default: 443). If you enter a port value, using the syntax `<hostname or IP address>:<port number>` then CipherTrust Transparent Encryption **does not** perform a port scan. CipherTrust Transparent Encryption uses the port number provided to verify the target server type using a TLS operation.

If you do not enter a port number, CipherTrust Transparent Encryption performs a port scan to check which ports are listening, including port 443.

Hardware Association Feature

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 clients.

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 client, 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 CipherTrust Manager.
4. Select **Enable hardware association** in the wizard.

Interactive Installation on Windows

The Windows interactive install uses a standard 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).

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

The following procedure describes how to install the CTE Agent on the host and then register the CTE Agent with a CipherTrust Manager..

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**.

Note

- 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** option is selected and click **Finish**.

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 Inst

Note

Thales supports installing or upgrading CTE 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
- Silent Installation Using the MSI File

Silent Installation Using the exe File

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a CipherTrust Manager using the exe file. To install silently using the MSI file or using the Microsoft System Center Configuration Manager (SCCM), see Silent Installation Using the MSI File.

Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured.
- CipherTrust Manager must contain a Client Profile. See Changing the Profile for more information.
- CipherTrust Manager must contain a registration token. See Creating a Registration Token.
- Optionally, the name of the host group that you want this client to be a member.
- CipherTrust Manager must contain an LDT Communication Group if you will use CTE to guard data over CIFS/NFS shares using LDT policies. See Managing LDT Communication Groupsfor more information.

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:

```
msiexec.exe /l* c:\temp\cte-install.log /i
<Installation_executable> /s /v /qn REGISTERHOSTOPTS="\Options\"
```

   where:

   - `/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.
- `ENABLE_LDT_CIFS=Yes` is an optional parameter that indicates you plan to use CTE-LDT with CIFS share GuardPoints on this host with a CipherTrust Manager. If you specify this option, you will *not* be able to guard any local directories on this host, even if those directories use a Standard CTE policy. Only CTE-LDT GuardPoints on CIFS shares will be supported for this host.
- `/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:

  CipherTrust Manager host name

  Required if you want to register CTE with a CipherTrust Manager.

  -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.

  -description

  Specifies a description for the host. This description is displayed in the CipherTrust Manager. If an entry for this host already exists, and the host already has a description, CipherTrust Manager **does not** overwrite the existing description, even if this option is specified.

  -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.

  -accessonly

  Enables access-only mode for LDT. (Default is full access mode.) In access-only mode, nodes are not be allowed to become part of an LDT Communication Group or

participate in data transformation, but they will continue to access a protected LDT CIFS GuardPoint.

-hostgroup

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

-log

Record installation steps in a log file.

-port=port

Specifies the port number this CTE Agent should use.

-profile

Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.

-silent

Make this a silent installation.

-token

The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.

-usehwsig

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

-useip

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

-vmd

Defines what kind of agent is being installed.

Note

If you want to enter an option with spaces in any value, it must be surrounded by 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 CipherTrust Manager host name is `my-key-mgr.example.com`.
- The CipherTrust Manager registration token is `12345` (`-token` parameter).
- 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.

```
msiexec.exe /l* /i vee-fs-7.3.0-135-win64.exe /s /v" /qn
INSTALLDIR=\"\"C:\cte\custom dir\"\" registerhostopts=\"my-key-
mgr.example.com  agent=my-host.example.com  token=12345
description=\"\"This host was silently installed\"\""
```

Example: LDT, LDT AccessOnly and Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the INSTALLDIR parameter is omitted).
- The CipherTrust Manager 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), LDT AccessOnly (`-accessonly`), and hardware association (`-usehwsig` parameter) features are enabled.

```
vee-fs-7.3.0-135-win64.exe /s /v" /qn
registerhostopts=\"my-key-mgr.example.com  token=12345 -useip -en
ableldt -accessonly -usehwsig\""
```

Example: LDT over CIFS/NFS

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the INSTALLDIR parameter is omitted).
- The CipherTrust Manager 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) and LDT Group (`-ldtgroup` parameter) features are enabled.

```
 vee-fs-7.3.0-135-win64.exe /s /v" /qn
       registerhostopts=\"my-key-mgr.example.com  token=12345 -u
seip -enableldt -ldtgroup=\"\"LDT-CG1\"\"
```

Silent Installation Using the MSI File

The following sections discuss how to install CTE for Windows silently and then register the CTE Agent with a CipherTrust Manager using the exe file. To install silently using the exe file, see Silent Installation Using the exe File.

Prerequisites

The following prerequisites must be met for CTE to install and register to CipherTrust Manager properly:

- CipherTrust Manager installed and configured.
- CipherTrust Manager must contain a Client Profile. See Changing the Profile for more information.

- CipherTrust Manager must contain a registration token. See Creating a Registration Token.
- Optionally, the name of the host group you want this client to be a part of.
- CipherTrust Manager must contain an LDT Communication Group if you will use CTE to guard data over CIFS/NFS shares using LDT policies. See Managing LDT Communication Groupsfor more information.

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:

```
msiexec.exe /i <Installation_executable> /qn INSTALLDIR=\"install-dir\" REGISTERHOSTOPTS="REGISTERHOSTOPTS_Options"
```

   where:

   - `/i` (required) enables CTE installation.
   - `ENABLE_LDT_CIFS=Yes` is an optional parameter that indicates you plan to use CTE-LDT with CIFS share GuardPoints on this host with a CipherTrust Manager. If you specify this option, you will not be able to guard any local directories on this host, even if those directories use a Standard CTE policy. Only CTE-LDT GuardPoints on CIFS shares will be supported for this host.
   - `/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:

CipherTrust Manager host name

Required if you want to register CTE with a CipherTrust Manager.

-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.

-description

Specifies a description for the host. This description is displayed in the CipherTrust Manager. If an entry for this host already exists, and the host already has a description, CipherTrust Manager **does not** overwrite the existing description, even if this option is specified.

-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.

-accessonly

Enables access-only mode for LDT. (Default is full access mode.) In access-only mode, nodes are not be allowed to become part of an LDT Communication Group or participate in data transformation, but they will continue to access a protected LDT CIFS GuardPoint.

-hostgroup

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

-log

Record installation steps in a log file.

-port=port

Specifies the port number this CTE Agent should use.

-profile

Specifies the client profile in the CipherTrust Manager that will be associated with this client. If this value is omitted, the CipherTrust Manager uses the default client profile.

-silent

Make this a silent installation.

-token

The registration token for the CipherTrust Manager with which you plan to register this client. Required for registration.

-usehwsig

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

-useip

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

-vmd

Defines what kind of agent is being installed.

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 CipherTrust Manager host name is `my-key-mgr.example.com`.
- The CipherTrust Manager registration token is `12345` (`-token` parameter).
- 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.

```
msiexec.exe /i vee-fs-7.3.0-135-win64.exe /qn
INSTALLDIR="C:\cte\custom dir" registerhostopts="my-key-mgr.example.com
agent=my-host.example.com  token=12345   description=\"This host was sil
ently installed\""
```

Example: CTE-LDT, LDT AccessOnly and Hardware Acceleration

The following example specifies that:

- The CTE Agent will be installed in the default installation directory (the INSTALLDIR parameter is omitted).
- The CipherTrust Manager 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), LDT AccessOnly (`-accessonly`), and hardware association (`-usehwsig` parameter) features are enabled.

```
msiexec.exe /i vee-fs-7.3.0-135-win64.exe /qn
registerhostopts="my-key-mgr.example.com  token=12345 -useip -
enableldt -accessonly -usehwsig"
```

Registering CTE After Installation is Complete

The following procedure describes how to register the CTE Agent after installation is complete.

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, to enable ransomware detection, and to register CTE on the CipherTrust Manager. After the host is registered, if you selected to enable file system encryption, you can configure CTE, apply GuardPoints, or perform database backups. If you selected ransomware protection, you can apply the protection to volumes. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

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 `...\register_host.exe -vmd -silent`.
3. Reboot the system. CTE automatically displays the registration wizard if CTE is not already registered.
4. In the Register Host dialog box, verify the host's machine name and click **Next**.
5. On the **Gathering agent information** page, select one or both of the following options and click **Next**.
   - **File System**: Allows you to protect and encrypt CTE files with policies
   - **Ransomware Protection**: Protects volumes from ransomware
6. On the **Gathering Key Manager information** page, enter the FQDN or IP address of the primary CipherTrust Manager.
   The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: **:**. For example:10.3.200.141:8445
   When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager to validate what features have been licensed and are available to the CTE Agent.
7. On the **Gathering host information** page:

   File System

   - Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.

- To prevent cloning, select **Enable Hardware Association**. For details, see Hardware Association Feature.
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the client, select **Enable LDT Feature**. For details on CTE-LDT, see **CTE-Live Data Transformation with CipherTrust Manager**.
- If you want the node to be an LDT AccessOnly node, select **Enable LDT AccessOnly Feature**.

Ransomware

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see Hardware Association Feature.

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

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

File System

- **Registration token**: The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name**: The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.
- **LDT Communication Group**: If you are planning on using LDT over CIFS/NFS on a CipherTrust Manager, enter the name of the LDT Communications Group that this node will join. See Adding Clients to an LDT Communication Group for more information.

Ransomware

- **Registration token**: The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name**: The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.

Warning

The registration information is case-sensitive. If any of it is entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client with the specified options. The Register Host dialog box displays a message with the results of the registration request.
If the registration completed successfully, click **Finish**.

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

          If you are using CipherTrust Manager version 2.1 or earlier, change the client password using the manual password creation method. This password allows

users to access encrypted data if the client is ever disconnected from the CipherTrust Manager. For details on changing the password, see the CipherTrust Manager documentation.

Using external certificates for communication between CTE Agent and CipherTrust Manager

Overview

CipherTrust Transparent Encryption can now use an external certificate, available at a user-defined path, to communicate with CipherTrust Manager.

Prerequisites

The external certificate must be:

- On the file system
- In PEM format

A key pair must already exist for the client:

- Must have Encryption type of either:
  - sha256WithRSAEncryption
  - ecdsa-with-SHA384
- Must be Encrypted with a pass phrase

Initial setup

1. Obtain your external CA certificate.
2. Create a certificate using the external CA certificate and key.

CipherTrust Manager Setup

To setup CipherTrust Manager to communicate through an external certificate:

1. Import the CA certificate into the CipherTrust Manager, click **CA** > **External** > **Add External CA**.

   Note

   In the Add External CA dialog, copy and paste the `<ca_certificate_name>`.pem file content from the UI page and provide a user-friendly name.

   For more information, see Using an Externally Generated Server Certificate for an Interface

2. Add the CA certificate to the list of trusted sources for the web interface, click **Admin Settings** > **Interfaces** > **web** > **Edit** > **External Trusted CAs**.
3. Restart the web server, click **Admin Settings** > **Services** > **web** > **Restart**.
4. Create a Registration Token for the CTE agent.

CTE Agent setup

1. Create a directory on the system to hold the required files, for example:
   - `/root/cert_files` (**Linux/AIX**)
   - `c:\temp\cert_files` (**Windows**)
2. Copy or create the following files in this directory:
   - **client_cert.pem**
   - **client_key.pem**
   - **passphrase** - this is currently expected as plain text
3. For **Linux/AIX** systems, to add the directory path to the environment, type:

```
$ export EXTERNAL_CERT_DIR=/root/cert_files
```

4. For **Windows** system, invoke registerhost.exe from the command line and add this argument:

```
c:\> register_host.exe -extcertdir=c:\temp\cert_files
```

5. Register the CTE client with the CM server as normal. If this is being done as part of an installation, then the above steps should be done before the installation, or, on windows, added to the registration parameters passed to the installer.

Post Registration

During registration, the certificate file is uploaded to the CipherTrust Manager, and the certificate and key files are imported into the CTE pem store. The key is decoded using the provided passphrase, then re-encoded using a random key using the normal CTE key security mechanisms for TLS keys. There is no need to keep the input files after registration is successful, so for security reasons they should be removed / shredded.

Certificate Renewal

The location of the external certificate files (i.e. the `EXTERNAL_CERT_DIR` or `-extcertdir` parameters) will be recorded in the CTE agent configuration file, `agent.conf`. When the current certificate is approaching expiration date (i.e. approx. 60 days prior to expiration) the CTE agent will look in this directory for an updated set of files.

If a new certificate file is present, then the file will be read and pushed to the CM, and if accepted, then the certificate and key will be imported into the CTE pem store, and the VMD process restarted to use the new certificate.

If no new certificate is present, a WARNING level message will be written to the logs and/or uploaded to the CM as per the logging settings, and the CTE agent will check again after 24 hours.

If the user wishes to change the directory path to store the new certificates, then the entry in the `agent.conf` file should be updated and the vmd service restarted. Alternatively, the user can update the external certificate set using the following command (this will not update the saved path):

```
    # vmutil -a vmd -d <ext_cert_Dir> updatecerts
```

If the user fails to update the certificate set prior to expiration then communication with the CM may be blocked, and re-registration will be required.

Note

Any renewed certificates must have exactly the same common name field as the original certificate, or the CipherTrust Manager will reject the update.

Validating CM and CTE with a Local CA Certificate

To ensure that registration by the CTE agent is serviced only by the expected key manager, you can provide a copy of the root CA certificate that will be used to authenticate the TLS communications with the key manager, during the registration process.

Note

You can only download the CA certificate when you are a root user in the root domain. You cannot download the certificate from a subdomain. It will not work.

Prerequisite

Make sure that you have previously created the client in CipherTrust Manager.

Using a Local CA Certificate

1. Extract the root CA certificate from the CipherTrust Manager.
    a. Log on to CipherTrust Manager as an administrator.
    b. In the left navigation pane, click **CA > Local**. The list of available CAs displays.
    c. Click the ellipsis icon corresponding to the CA.
    d. Click **Download** to download the CA.
    e. Copy the certificate to a directory on the agent system.
2. To install the root CA certificate into the CTE client, add it to the registration command line:

Note

You must have administrator privilege to complete this step.

C:\Windows\system32> C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe -silent -log= -vmd -agent= -token= -cafile=

Example

```
C:\Program Files\Vormetric\DataSecurityExpert\agent\shared\bin\register_host.exe -silent -log=c:\vte_reg_log.txt -vmd 10.171.36.175 -agent=ani-vm-217-35190.sjcicd.com -token=mMEz3Y6Ob9D4L7QuvK5SOmhulRm8DYI8odV5j3OdvuHqk6LhZqE0FeIZHILYTmDiE9 -cafile=C:\tmp\Austin175.pem
```

3. Confirm in CipherTrust Manager that the client is registered and healthy.

Setting the CM log for Ransomware Protection

Setting the CipherTrust Manager log for Ransomware Protection

You need to configure the logging level on CipherTrust Manager to INFO instead of the default, which is ERROR.

To define client log configurations for a profile:

1. Open the **Transparent Encryption** application.
2. In the left pane, click **Settings** > **Profiles**.
3. Click on the name of the relevant profile.
4. Click **CLIENT LOGGING CONFIGURATION** to expand it.
5. Set the **Log Level** to **INFO**.

6. Click **Update**. The changes are effective immediately and apply to the clients linked with the profile.

The CTE client logs can be seen on the **Records** > **Client Records** page of the CipherTrust Manager GUI. Filter the records by **Client Type** and look for the **CTE** records.

Multifactor Authentication for CTE GuardPoints

CipherTrust Transparent Encryption is supporting Multifactor Authentication through integration with various MFA providers. CipherTrust Transparent Encryption will continue to integrate with additional providers.

- Introduction to Multifactor Authentication
- Current Compatible Multifactor Authentication Providers
- Use Cases for Multifactor Authentication
- Exempting some users from authentication with a Whitelist
- Remote Authentication for Multifactor Authentication
- Administration for Multifactor Authentication
- Troubleshooting Multifactor Authentication

Introduction to Multifactor Authentication

Why do companies need Multifactor Authentication

Every day, the threat of ransomware attacks increase in frequency, sophistication, and effectiveness. Victims of ransomware attacks can be blocked from data, applications, and systems – making an organization unable to function.

Credential compromise is the leading cause of ransomware attacks, because credentials give hackers the access they need to hold your systems hostage. Unfortunately, credentials can be stolen, shared, bought or hacked. Once the hackers

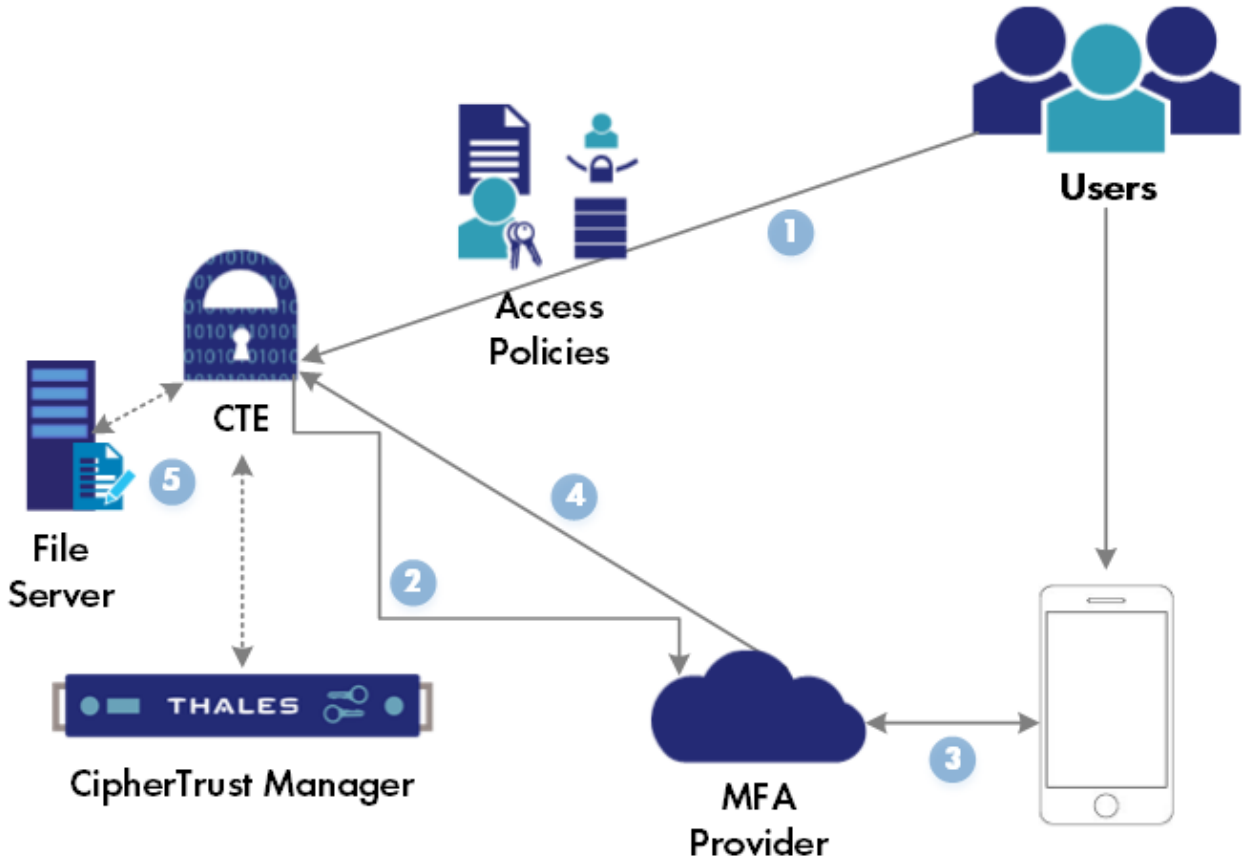
gain entry, the threat actors will often look to compromise privileged access credentials to further infiltrate your network and steal sensitive data.

What is Multifactor Authentication

Multifactor authorization ensures that the access credentials presented belong to the actual person. After logging in to the system, when a user tries to access a CipherTrust Transparent Encryption GuardPoint, it triggers a second factor authorization to verify the user with a second form of authentication, like sending a passcode to the users's registered cell phone, that they then have to input into the application.

How does Multifactor Authentication work

The following diagram explains how Multifactor Authentication operates in a CipherTrust Transparent Encryption environment.



Step	Description
1	Multifactor Authentication is performed when a user tries to access a file in a GuardPoint.

Step	Description
	NOTE: Multifactor Authentication is only enforced when a file, in a GuardPoint, is first accessed by the user. Multifactor Authentication is not enforced during IO activity, (read/write requests). Therefore, if the file has already been opened by a user/application, Multifactor Authentication will not be enforced on that file.
2	CipherTrust Transparent Encryption sends a message to the Multifactor Authentication provider to verify the user.
3	Multifactor Authentication provider sends a verification request to the user's registered device. **NOTE**: If Multifactor Authentication is using Password Authentication, this step is not required.
4	Multifactor Authentication provider confirms/denies user access.
5	If authenticated, user has access to the MFA-enabled GuardPoint based on the CipherTrust Transparent Encryption access policy. If denied, user does not gain access to the GuardPoint.

For more information on Multifactor Authentication, see Multifactor Authentication.

Compatible MFA Providers

Thales will be continually adding new MFA providers to CipherTrust Transparent Encryption. When the MFA providers pass compatibility testing, they will be added to this page. Select the MFA provider that you are using and follow the instructions below to set up CipherTrust Transparent Encryption for the MFA.

- Safenet Trusted Authentication
- OKTA
- KeyCloak
- Cisco DUO
- Microsoft Azure Entra ID Support

Using STA for Multifactor Authentication for CTE GuardPoints

Prerequisites

- Have a CipherTrust Manager set up with:
  - Client Profile enabled for Multifactor Authentication
  - Registration token
- Integrate with Safenet Trusted Access by creating and managing your access controls in Safenet Trusted Access.

Selecting the Proper Template

> **Note**
>
> Make sure that, in Safenet Trusted Access, you choose the custom template: **CTE_OIDC**.

If the **CTE_OIDC** template is not available in your account:

1. Create an app using the **Generic Template**.
2. For the Integration Protocol, select **OIDC**.
3. Configure **VALID REDIRECT URL** as: http://127.0.0.1:5560/auth/callback.

> **Note**
>
> Port 5560 is the default CTE OIDC login port. If the CTE admin changes it through the `voradmin mfa` command, you must chang that value in the redirect URL.

Create an OIDC Connection with CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management** > **Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

   Note

   Refer to your Multifactor Authentication provider profile for the values:

   - **URL of OIDC provider:**

     Linux

     - **For KeyCloak, select the URL of the OIDC provider**

     Windows

     - For Thales Safenet Trusted Access, select **Well Known Configuration URL**
     - For all other providers, select the URL of the OIDC provider

   - Client-ID as configured for the OIDC client
   - Client-Secret as shown for the OIDC client
7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

For more on the Safenet Trusted Access OIDC template, see OIDC applications.

Using Okta for Multifactor Authentication for CTE GuardPoints

Integration with Okta requires creating an OIDC connection in CipherTrust Manager, after you create an OIDC template in Okta.

Prerequisites

- Have a CipherTrust Manager set up with:
  - Client Profile enabled for Multifactor Authentication
  - Registration token

On the Okta platform

1. Create an admin user.
2. Create one or more Okta users. **Note** that Okta requires the username to be in email format.
   - Create **domain users** in the format: `<username>@<domain>.com`
   - Create **host specific users** in the format: `<username>@<hostname>.com`
   - Create **non-domain users** in the format: `<username>@localhost.com`.

   Non-domain users map to system users with implicit host domain access on each host.
3. Create an OIDC application (“App Integration”) with the following settings:
   - **Application type**: Web Application
   - **Client Authentication**: Client Secret
   - **Grant type**: Authorization Code
   - **Login/Sign-in Redirect URIs**: `http://127.0.0.1:<CTE-OIDC-Login-Port>/auth/callback`
   - **Default value of CTE-OIDC-Login-Port**: 5560, if CTE admin changes this port, they must provide the updated value.

4. Note the OIDC parameters:
    - Client-ID as configured for the OIDC client
    - Client-Secret as shown for the OIDC client

On CipherTrust Manager

The Provider Url for the Okta account is in the following format:

```
https://<okta-account>.okta.com/.well-known/openid-configuration
```

Create an OIDC connection on CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management** > **Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

> **Note**
>
> Refer to your Multifactor Authentication provider profile for the values:

- **URL of OIDC provider:**

Linux

- **For KeyCloak, select the URL of the OIDC provider**

Windows

- For Thales Safenet Trusted Access, select **Well Known Configuration URL**
- For all other providers, select the URL of the OIDC provider

- Client-ID as configured for the OIDC client

- Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Using Keycloak for Multifactor Authentication for CTE GuardPoints

Integration with Keycloak requires creating an OIDC connection in CipherTrust Manager, after you create an OIDC template in Keycloak.

Prerequisites

- Have a CipherTrust Manager set up with:
  - Client Profile enabled for Multifactor Authentication
  - Registration token
  - CipherTrust Transparent Encryption host and Keycloak server must have their time's synchronized. If they are not time-synced, then Multifactor Authentication login fails with the following error:

    ```
    Failed to verify ID Token: oidc: token is expired (Token Expiry: 2022-11-08 22:42:20 -0800 PST)
    ```

On the Keycloak platform

1. Create an admin user.
2. Login to the realm and create one or more users.
3. Create a password for the user.
4. Create an OIDC client in realm with the following settings enabled:
   - **Valid Redirect URIs**: Configure in the format:

     ```
     http://127.0.0.1:<CTE-OIDC-Login-Port>/auth/callback
     ```

   - **Default value of CTE-OIDC-Login-Port**: 5560, if CTE admin changes this port, they must provide the updated value.

- **General Settings**:
  - **Client Type**: OpenID Connect
  - **Client ID**: Client name
- **Capability Config**:
  - **Client Authentication**: On
  - **Authorization**: On
  - **Authentication Flow**: Standard Flow

5. Note three OIDC parameters:
   - Provider URL format:
     - For **non-TLS**: `http://<keycloak-ip>:<keycloak-port>/realms/<realm-name>/.well-known/openid-configuration`
     - For **TLS**: `https://<keycloak-ip>:<keycloak-port>/realms/<realm-name>/.well-known/openid-configuration`

     Note

     If KeyCloak is configured for TLS, the KeyCloak certificate (if self-signed), or certificate chain, including the root CA, and any intermediate CAs, must be imported into the CipherTrust Transparent Encryption client machine. Import the self-signed certificate as a root CA. CipherTrust Transparent Encryption will fail to connect to the provider if certificates are not imported. To import a certificate: see Importing Certificates Using MMC
   - Client-ID as configured for the OIDC client
   - Client-Secret as shown for the OIDC client

Create an OIDC connection on CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management** > **Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.

6. Enter values for the configuration information.

> **Note**
>
> Refer to your Multifactor Authentication provider profile for the values:

   - **URL of OIDC provider:**

Linux

   - **For KeyCloak, select the URL of the OIDC provider**

Windows

   - For Thales Safenet Trusted Access, select **Well Known Configuration URL**
   - For all other providers, select the URL of the OIDC provider

   - Client-ID as configured for the OIDC client
   - Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Using Cisco DUO for Multifactor Authentication for CTE GuardPoints

Integration with Cisco DUO requires creating an OIDC connection in CipherTrust Manager, after creating a DUO account.

On the DUO platform:

1. Create an account on Cisco Duo.
2. Login to your Cisco DUO account as an admin and click **Users** in the left navbar to create/add one or more users.

3. While creating a user, set the **Status** as **Active**
4. Click **Applications** in the left navbar.
5. Click **Protect an Application**.
6. In the search field, type **Web SDK**.
7. In the Web SDK field, click **Protect**.
8. In the application created, note the values for:
    - **Client ID**
    - **Client Secret**
    - **API hostname**

> **Note**
>
> https:// is the value for the URL of the OIDC Provider.

Create an OIDC Connection with CipherTrust Manager

1. Log on to the CipherTrust Manager GUI as an administrator.
2. In the left pane, click **Access Management** > **Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values for the configuration information.

> **Note**
>
> Refer to your Multifactor Authentication provider profile for the values:

    - **URL of OIDC provider:**

Linux

- **For KeyCloak, select the URL of the OIDC provider**

Windows

- For Thales Safenet Trusted Access, select **Well Known Configuration URL**
- For all other providers, select the URL of the OIDC provider

- Client-ID as configured for the OIDC client
- Client-Secret as shown for the OIDC client

7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Using Microsoft Azure Entra ID Multifactor Authentication for CTE GuardPoints

Create an OIDC Application in Entra ID

1. Select **Microsoft Entra ID** from your Azure Homepage.
2. Click **App Registration**.
3. Create a **New Registration**.
4. Record the client ID. You will need it when you create an OIDC connection on CipherTrust Manager.
5. Click **Certificates and Secrets** in the left Nav bar.
6. Create a new **Client Secret**. This is the Client Secret value that you will enter in CipherTrust Manager.
7. For the Redirect URI, select **Web**.

8. Enter redirect URL with your local host name: `http://<localhost>:5560/auth/callback` and save it.
9. Click on the name of your registration and click **Endpoints**.
10. Copy the value for the Endpoint for **OpenID Connect metadata document**. This is the OIDC Provider value that you will enter in CipherTrust Manager.

Create an OIDC Connection in CipherTrust Manager

1. Log on to the CipherTrust Manager as an administrator.
2. In the left pane, click **Access Management** > **Connections**.
3. In the Connections, click **Add Connection**.
4. Click **OIDC** and then click **Next**.
5. Provide a name for the connection and click **Next**.
6. Enter values collected in the previous section for the configuration information.
    - OIDC Provider:

      `<value for the Endpoint for OpenID Connect metadata document>`
    - Client ID
    - Client Secret
7. Click **Next** and in the Add Products window, select **CTE** for product.
8. Click **Add Connection**.

Set Client Profile in CipherTrust Manager

1. In CipherTrust Manager, open the Transparent Encryption application.
2. In the left pane, click **Settings > Profiles**.
3. Select the desired client profile.
4. Expand **MULTIFACTOR AUTHENTICATION**.

5. Select the OIDC Connection that you created for Entra ID.
6. Select **MFA Exempted User Set** from the drop-down list. This user set will be exempted from MFA so MFA will not be enforced on the users of this set. See Exempting some users from authentication with a Whitelist for more information.

Domain Mapping

Domain mapping is required for Entra ID. If you try to log in prior to mapping the domain, CTE generates an error.

You must map the domain **from** the Entra ID domain **to** the domain of the existing CTE host. Ask your System Administrator for the domain information.

1. To set the domain, type:

```
voradmin mfa domains-map set <domain1>:<domain2>
```

Example

```
voradmin mfa domains-map set thalesgroup.com:qa.com
```

Response

```
Restart secfsd service to affect changes.
```

> **Note**
>
> You can map multiple domains using a comma in between domain names. For example:
>
> ```
> voradmin mfa domains-map set <domain-1-onMFA-provider>:<domain-1-onHost>,<domain-2-onMFA-provider>:<domain-2-onHost>
> ```

2. To stop secfsd, type:

```
net stop secfsd
```

3. To restart secfsd, type:

```
net start secfsd
```

Use Cases for MFA on CTE

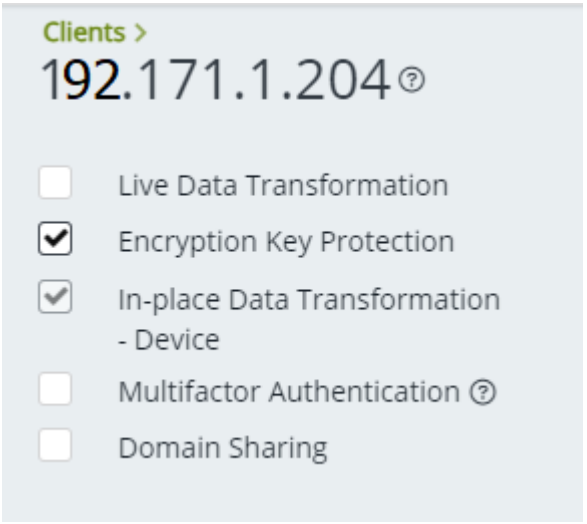
When using Multifactor Authentication with CipherTrust Transparent Encryption, after successfully completing the MFA provider, you can enable it on a:

- Client
- GuardPoint
- GuardPoint, while exempting certain users/applications/processes from authentication

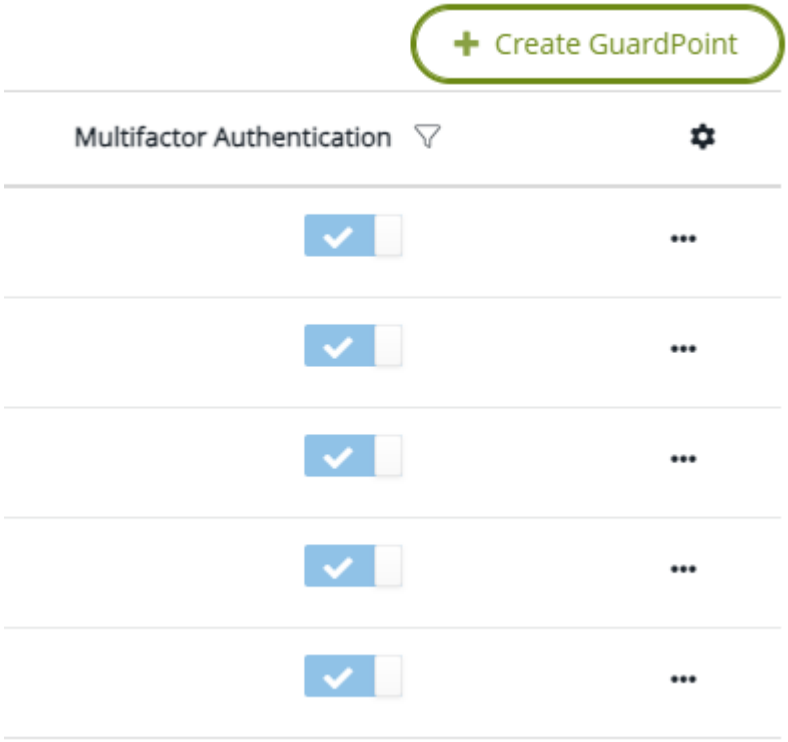
Enable Multifactor Authentication on a client

You can enable Multifactor Authentication for all of the GuardPoints on a client. When Multifactor Authentication is enabled at the client level, CTE enforces the configuration for all GuardPoints configured on the client. It overrides any MFA configuration set for individual GuardPoints.

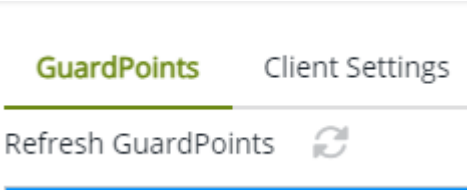
1. Open **CipherTrust Manager > Transparent Encryption** application.
2. Select the relevant client.
3. In the upper pane, select **Multifactor Authentication**.



4. Select **Apply**. All of the Multifactor Authentication switches are toggled to the **on** position.



5. If the MFA column doesn't display with all switches set to on, click **Refresh GuardPoints** to display the Multifactor Authentication column.



Note

To disable Multifactor Authentication on a GuardPoint, deselect Multifactor Authentication in the upper pane and click **Apply**.

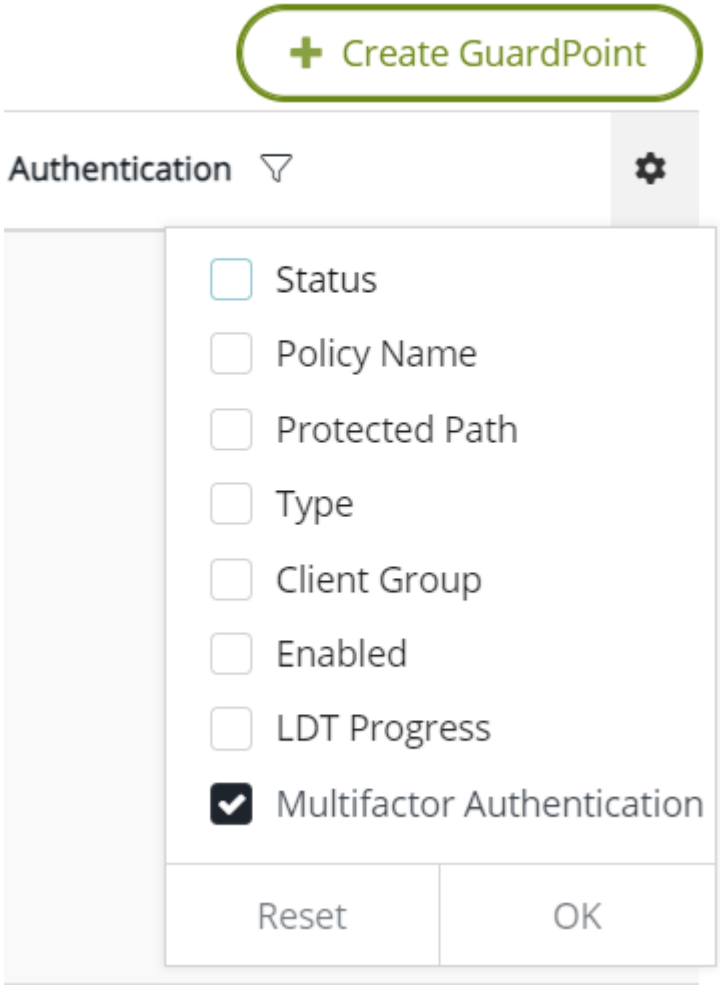
Enable Multifactor Authentication on a GuardPoint

You can enable Multifactor Authentication for individual GuardPoints on clients.

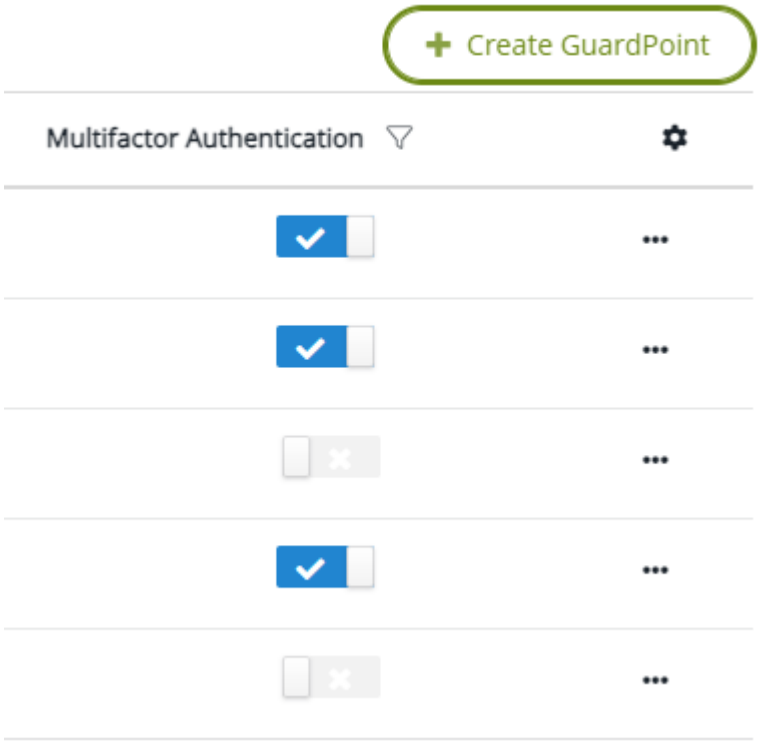
1. Open **CipherTrust Manager > Transparent Encryption** application.
2. Select the relevant client.
3. Select the **GuardPoints** tab.

4. Click the settings icon.

5. Select **Multifactor Authentication** to enable Multifactor Authentication for the GuardPoints.



6. Click **OK**. The Multifactor Authentication column displays.



7. Toggle the Multifactor Authentication switch to enable Multifactor Authentication for the selected GuardPoints.

Note

To disable Multifactor Authentication on a GuardPoint, deselect the Multifactor Authentication toggle switches.

Enable Multifactor Authentication for Client Groups

Multifactor authentication cannot be enabled at the client group level. However, you can enable Multifactor Authentication for individual GuardPoints on client groups.

While propagating the Multifactor Authentication-enabled GuardPoints to the member clients, CipherTrust Transparent Encryption checks the Multifactor Authentication capability of the member clients. If a client is Multifactor Authentication-capable, the GuardPoints are added to the client. If a client is not Multifactor Authentication-capable, the GuardPoints are skipped.

Exempting some users or processes from authentication with a Whitelist

When you activate CTE Multifactor Authentication, all users attempting to log in to the CTE client must successfully pass through CTE Multifactor Authentication to gain entry to the MFA-enabled GuardPoints. However, there are specific exemptions to this rule. Users whose system services, or applications, initiate automatically during system boot-up cannot undergo authentication though CTE Multifactor Authentication, as Multifactor Authentication necessitates user interaction. To accommodate such cases, exempt these users from Multifactor Authentication enforcement within the Client Profile by including them in the user set exemption list. Typically, only system users responsible for running system services are included in this list. However, since many system applications operate under the root user, or even under normal application user accounts, you must also add these system administrator/application users to the list. These users form part of the user set, commonly referred to as a whitelist.

Caution

Be careful when adding a user to the whitelist. The exemption applies for the entire client. Users on this list can bypass Multifactor Authentication and access all MFA-enabled GuardPoints. If a system service, or application, accesses only one GuardPoint among multiple GuardPoints, Thales advises you to leave that specific GuardPoint without Multifactor Authentication enforcement.

Note

You **cannot** share the whitelist between Windows and Linux operating systems. Each client profile must contain a unique Multifactor Authentication whitelist. Therefore, the User Set contains different users in Windows and Linux platforms. A CTE Windows client and a CTE Linux client **cannot** share the same client profile when Multifactor Authentication is enabled.

Creating a User Set

See Creating User Sets for information on creating a User Set in a Policy Element.

Adding the User Set to the Client Profile

To add an Multifactor Authentication whitelist to the client profile:

1. Create your Client Profile if it is not already created.
2. Click on your client profile to open it.
3. Click **Multifactor Authentication**.
4. In the **Select OIDC connection** field, select the OIDC connection that you created.
5. In the **Select the MFA exempted User Set** field, select the User Set that contains the people/applications that are exempted from authorization.
6. Click **Update**.

Remote Authentication for Multifactor Authentication

By default, CipherTrust Transparent Encryption works with a local Multifactor Authentication login. In CipherTrust Transparent Encryption v7.6 and subsequent versions, you can configure remote authentication for Multifactor Authentication. This allows a user to log into Multifactor Authentication through a machine other than a CTE client. This allows you to enable authentication from remote endpoints accessing CIFS shares, exported by a CTE agent.

Note

- Your Windows remote access system logon account name, and your Multifactor Authentication account name, **MUST** be the same.
- The MFA username, including the domain-name, in the format domain\username or username@hostname, must exist on the MFA provider.

Remote Authentication configuration requires a non-encrypted private key and certificate. The CipherTrust Transparent Encryption OIDC service uses the key and certificate for TLS communication. CTE stores encrypted keys and certificates internally.

Prerequisites

- Create a firewall rule on a CTE agent to allow all incoming TCP traffic on the Multifactor Authentication login port.
- Generate a private key and certificate. You must know the name and location of these files.
- In the Keycloak setup, set the **redirect-url** parameter for OIDC configuration using the following format: `https://<cte-hostname>:<mfa login port>/auth/callback`.

> **Note**
>
> ◦ The Administrator can choose to use a wildcard ('*'), if the same configuration is reused across many CTE agents.

- You must have administrator access so that you can restart secfsd service:

  1. To stop secfsd service, type:
     net stop secfsd
  2. To start secfsd service, type:
     net start secfsd

Starting Remote Authentication for Multifactor Authentication

To configure remote authentication:

1. In a command line, type:

```
voradmin mfa remote-config set [<privateKeyFile>
<certificateFile>]
```

Example

```
voradmin mfa remote-config set private-key.pem cert.pem
```

Response

```
voradmin mfa remote-config set
Restart secfsd service to affect changes.
```

2. Restart the secfsd service.

Disabling Remote Authentication for Multifactor Authentication

To disable remote authentication:

1. In a command line, type:

```
voradmin mfa remote-config unset
```

Response

```
Restart secfsd service to affect changes.
```

2. Restart the secfsd service.

Validating Certificate and Private files information

To validate the two certificates:

- In a command line, type:

```
voradmin mfa remote-config get [<privateKeyFile>
<certificateFile>]
```

Example

```
voradmin mfa remote-config get private-key.pem cert.pem
```

Response

```
sha256 of key file:
dcb8eXXXXa92ac5dff34aXXXXab3811245aXXXXc204733bbead43f4846274674

sha256 of certificate file:
3e2eec5bXXd357d14f5c0047d36aXXXXXXXfc87f2a74ca3b5c2c2627XXXe6db4

certificate:
-----BEGIN CERTIFICATE-----
MIIFuTCCA6GgAwIBAgIUR+Gh3z7J8TzQr6buZGDcK9h/8MQwDQYJKoZIhvcNAQEL
BQAwbDELMAkGA1UEBhMCSU4xCzAJBgNVBAgMAlVQMQswCQYDVQQHDAJOTzEMMAoG
A1UECgwDQ1BMMQwwCgYDVQQLDANESVMxCzAJBgNVBAMMAlRIMRowGAYJKoZIhvcN
.
.
.
/31kjs/Kms582KTKFKFqzuZHJ4L6odL6JBOmbvv4UZGB2t99ah0R9BAutivru/0M
ZFvotV9Xsxs49PtOgj1vkWFdlWUR7VtcdfOtiIoSvuXhMjCvTq8KtPIXiJJjFFkN
3xD4ZmG7M14u1hzmaXqHfZ02YZOISFltq2PUWqQ=
-----END CERTIFICATE-----
```

Using Remote Authentication for Multifactor Authentication

To login and use Multifactor Authentication from a remote endpoint:

- User must open a browser and enter a valid URL with the format: `https://<cte-hostname>:<mfa login port>/login`.

> **Note**
>
> When launched from the Etray application on a CTE agent, the browser is launched with the required URL automatically in the URL field.

Administrator Tasks for Multifactor Authentication

Using the Proper Filter

Note

The Multifactor Authentication feature **requires** the CTE `VMLFS` driver. This driver **must** be running in order for Multifactor Authentication to work.

- All new installations of 7.3.0.x contain this driver. Type `fltmc` to verify. A table displays listing all current drivers.

Filter Name	Num	Instances	Altitude	Frame
WdFilter		4	328010	0
storqosflt		0	244000	0
wcifs		0	189900	0
vmlfs		4	142900	0
FileCrypt		0	141100	0
luafv		1	135000	0
npsvctrig		1	46000	0
Wof		1	40700	0

- Agents upgraded from 7.2.0, and previous versions, may be using the vmfiltr driver. If the agent ran the vmfiltr driver, then when you upgrade to 7.3.0, it will start with the vmfiltr driver. If the previous agent ran the vmlfs driver, then when you upgrade to 7.3.0, it will start the vmlfs driver. Type the following to switch to the vmlfs driver:

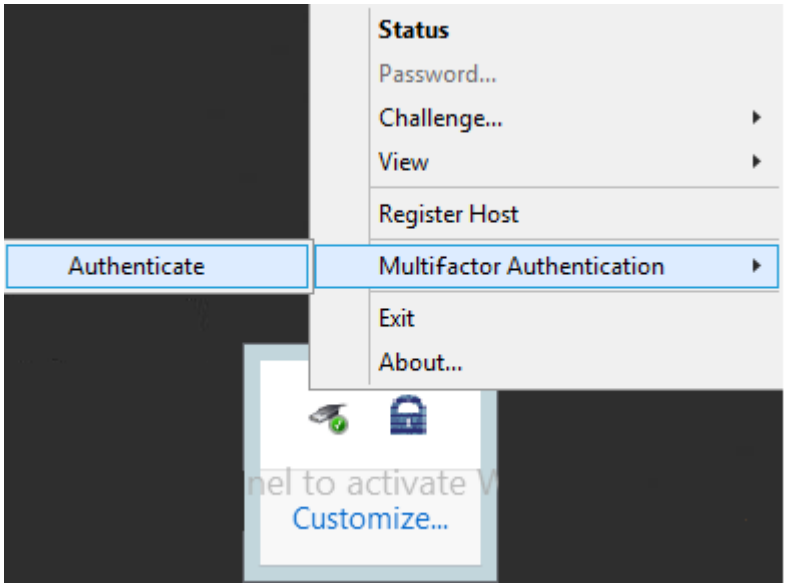
```
voradmin config enable vmlfs
```

User Authentication

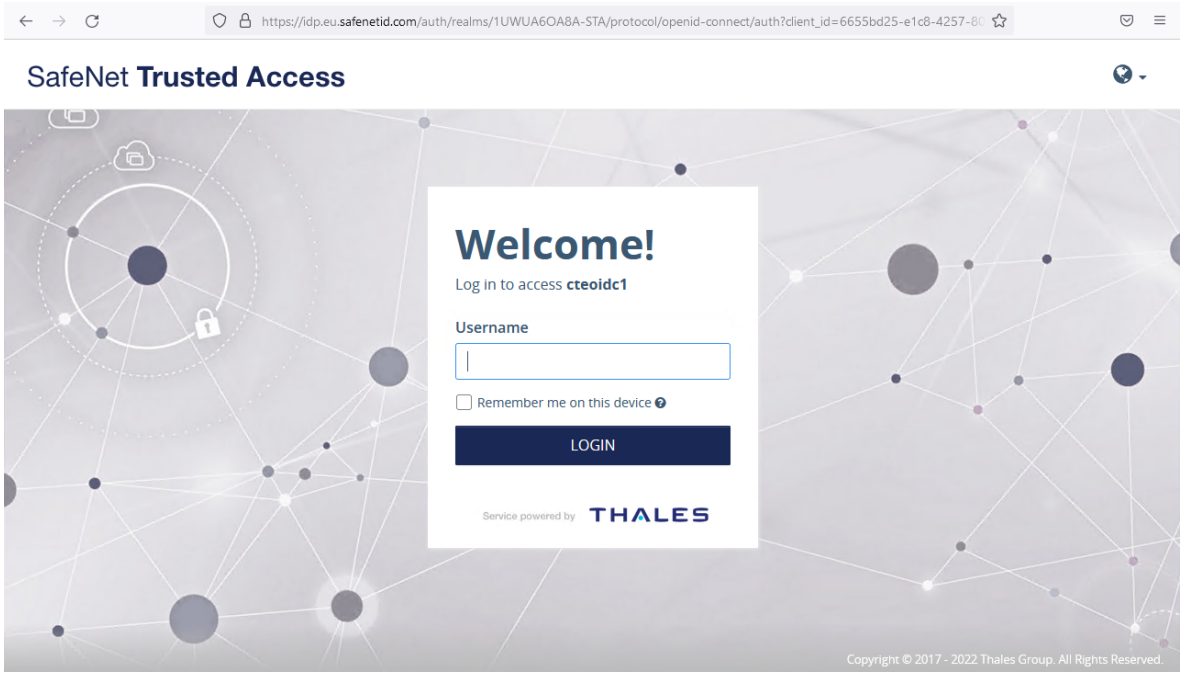
Authentication is provided for the entire client and is enforced the first time a user opens a file. After the initial file opening, the user can perform read/writes to the file.

To authenticate, a user can login to MFA from the Windows system tray:

1. Click on the CTE icon in the System Tray.
2. Select **Multi-Factor Authentication** > **Authenticate**.



3. Login in to access the STA OIDC template.



After you log in, a message displays confirming your authentication and your access to the GuardPoint.

4. Close the Window to continue.

Note

If you logout, you disable your access to the GuardPoint.

Voradmin Commands

voradmin mfa status

Displays the MFA information for a user.

Syntax

```
voradmin mfa status
```

Example

```
C:\Windows\system32>voradmin mfa status
```

Response

```
User \dram is allowed access.
MFA enabled guardpath(s) (Number of paths: 2):
C:\cm\gp2
C:\cm\gp1
```

voradmin mfa config

Displays configuration information.

Syntax

```
voradmin mfa config
```

Response

```
HostMfaEnable is set.
MFA enabled guardpath(s) (Number of paths: 2):
C:\cm\gp2
C:\cm\gp1
MFA access allowed users(s) (Number of users: 2):
    Users\dram
    NT AUTHORITY\SYSTEM
MFA Exempt-List: (Number of entries: 1)
    user: "system", group: "", domain(s): "NT AUTHORITY"
OIDC configuration:
    login-port : 5560
    notification-port : 5562
    client-id : 6653gd25-e1c7-4257-6034-46c77ffc8cb6
            url : https://idp.eu.safenetid.com/auth/realms/
1UWUA52A8A-STA
```

voradmin mfa check-connection

Allows the admin user to check the connection to the OIDC provider.

Syntax

```
voradmin mfa check-connection <name_of_OIDC-configuration-url>
```

Example

```
C:\Windows\system32>voradmin mfa check-connection https://
idp.eu.safenetid.com/auth/realms/1UWUA6OA8A-STA/.well-known/openid-
configuration
```

Response 1: Success

```
Connection ok to https://idp.eu.safenetid.com/auth/realms/
1UWUA6OA8A-STA/.well-known/openid-configuration
```

Response 2: Failure

```
Connection failed to https://idp.eu.safenetid.com/auth/realms/
1UWUA6OA8A-STA/.well-known/openid-configuration-bad
```

voradmin mfa update-ports

Allows the administrator to update the OIDC ports.

- Updating the ports restarts the CipherTrust Transparent Encryption Multifactor Authentication application. Users must login to Multifactor Authentication again after the ports are updated.

Warning

If the OIDC-login-port is changed, then the redirect-URI for the OIDC application at the Multifactor Authentication provider must also be changed. It is specified in the format: `http://127.0.0.1:<oidc-login-port>/auth/callback`. If redirect-URI is not changed, CipherTrust Transparent Encryption may fail to connect to the provider.

Syntax

```
voradmin mfa update-ports <oidc-login-port> <oidc-notification-port>
```

Example

```
C:\Windows\system32> voradmin mfa update-ports 8000 8075
```

Response

```
Updated OIDC ports
```

voradmin mfa set-auth-expiry

Allows the admin to set an authentication expiry time.

Note

Changing authentication expiry clears all existing MFA logins. Users must login again.

Syntax

```
voradmin mfa set-auth-expiry <time interval in minutes (specify 0 to disable expiry time)>
```

Example

```
C:\Windows\system32> voradmin mfa set-auth-expiry 5
```

Response

```
Authentication will expire every 5 minute(s).
Re-authenticate for new settings.
```

voradmin mfa localhost-redirect-uri

You do not need to manually set a parameter for this command. If you use `set` it automatically uses `http://localhost:5590/auth/callback` as the redirect URI. If you use `unset` it automatically uses the default redirect URI for the MFA provider. This command is useful if an MFA provider does not allow 127.0.0.1 as the redirect URI.

Syntax

```
voradmin mfa localhost-redirect-uri <get|set|unset>
```

voradmin mfa domains-map

Domain mapping is generally applicable for use with all providers, though it is only required for Entra ID.

Syntax

```
voradmin mfa domains-map <get|set|unset> <domain1>:<domain2>
```

Example

```
voradmin mfa domains-map set thalesgroup.com:<localhost>.com
```

Response

```
Restart secfsd service to affect changes.
```

Note

You can map multiple domains using a comma in between domain names. For example:

```
voradmin mfa domains-map set <domain-1-onMFA-provider>:<domain-1-onHost>,<domain-2-onMFA-provider>:<domain-2-onHost>
```

voradmin mfa remote-config

Remote authentication allows a user to log into Multifactor Authentication through a machine other than a CTE client. This allows you to enable authentication from remote endpoints accessing CIFS shares, exported by a CTE agent.

Syntax

```
    voradmin mfa remote-config [<get|set|unset>] [<privateKeyFile> <certificateFile>]
```

Options	Description
certificateFile	Presented to web browser during TLS communication to the web browser.
get	Displays the 'sha256' encryption for keys and certificates. It allows the customer to check for a valid key and certificate that they imported using the `set` option.
privateKeyFile	Used by the OIDC service for TLS communication with the web browser.

Options	Description
set	Imports the key and certificate in use by CTE.
unset	Disables the remote authentication for Multifactor Authentication and reverts back to local Multifactor Authentication authentication.

See Remote Authentication for Multifactor Authentication for more information.

Restarting SecFSD

Many Multifactor Authentication commands require restarting SecFSD to enable.

1. To stop secfsd, type:

```
net stop secfsd
```

2. To restart secfsd, type:

```
net start secfsd
```

Choosing a Login Name Type

Currently, CipherTrust Transparent Encryption authenticates users with a User Principal Name (UPN). In Windows Active Directory, a UPN is the name of a system user. It is written in an email address format, for example: john.doe@domain.com.

The Security Account Manager (SAM) is a Windows database that stores user accounts and security descriptors for users on the local computer. The SAM Account Name is used to support clients and servers running earlier versions of the operating system, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager.

Previously, CipherTrust Transparent Encryption only supported the UPN. Now, you can choose which login name you want your users to use. However, you must choose SAM Account Name or UPN. You cannot use both. By default UPN support is enabled on a host.

CipherTrust Transparent Encryption provides the following `voradmin` commands to change the Windows registry entries.

To enable SAM support:

1. Type the following command:

```
voradmin config usernamesupport samAccountName
```

2. Reboot the system for the changes to take affect.

To enable UPN support:

1. Type the following command:

```
voradmin config usernamesupport userPrincipalName
```

2. Reboot the system for the changes to take affect.

To get a status of the current support:

1. Type the following command:

```
voradmin config usernamesupport getCurrentNameSupport
```

2. Reboot the system for the changes to take affect.

Ransomware Protection

- Setting up Ransomware Protection during Registration
- Use Cases for Ransomware Protection
- Creating GuardPoints for Ransomware Protection

Registration with Windows

The following procedure describes how to register the CTE Agent after installation is complete.

Use the `register_host` utility to create certificate requests, exchange certificates between the CipherTrust Manager and the host, to enable ransomware detection, and to register CTE on the CipherTrust Manager. After the host is registered, if you selected to enable file system encryption, you can configure CTE, apply GuardPoints, or perform

database backups. If you selected ransomware protection, you can apply the protection to volumes. Run the `register_host` utility in text mode on a terminal window.

Caution

The default host registration timeout is 10 minutes. If the host is unable to reach the CipherTrust Manager within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You might also have to extend the default TCP timeout.

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 `...\register_host.exe -vmd -silent`.
3. Reboot the system. CTE automatically displays the registration wizard if CTE is not already registered.
4. In the Register Host dialog box, verify the host's machine name and click **Next**.
5. On the **Gathering agent information** page, select one or both of the following options and click **Next**.
   - **File System**: Allows you to protect and encrypt CTE files with policies
   - **Ransomware Protection**: Protects volumes from ransomware
6. On the **Gathering Key Manager information** page, enter the FQDN or IP address of the primary CipherTrust Manager.
   The default communication port is 443. If you want to specify a different communication port, enter it with the primary key manager host name in the format: **:**. For example:10.3.200.141:8445
   When you are done, click **Next**. CTE communicates with the selected CipherTrust Manager to validate what features have been licensed and are available to the CTE Agent.
7. On the **Gathering host information** page:

File System

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see Hardware Association Feature.
- If you want to have CipherTrust Transparent Encryption - Live Data Transformation available on the client, select **Enable LDT Feature**. For details on CTE-LDT, see **CTE-Live Data Transformation with CipherTrust Manager**.
- If you want the node to be an LDT AccessOnly node, select **Enable LDT AccessOnly Feature**.

Ransomware

- Specify the host name or IP address of the client. You can select the host name from the drop-down list or type it in the field.
- To prevent cloning, select **Enable Hardware Association**. For details, see Hardware Association Feature.

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

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

File System

- **Registration token**: The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name**: The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.
- **LDT Communication Group**: If you are planning on using LDT over CIFS/NFS on a CipherTrust Manager, enter the name of the LDT Communications Group that this

node will join. See Adding Clients to an LDT Communication Group for more information.

Ransomware

- **Registration token**: The registration token for the CipherTrust Manager with which you want to register this host.
- **Profile name**: The name of the profile that you want to associate with this host. This name must match exactly the name of the profile in the CipherTrust Manager. If you do not specify a profile name, the CipherTrust Manager associates the default client profile with this client.
- **Host group** (optional): The name of the client group to which the client will be added.
- **Host description** (optional): A user-defined description of the client. This description will be displayed in the CipherTrust Manager.

Warning

The registration information is case-sensitive. If any of it is entered incorrectly, the client registration will not succeed. If the registration fails, click Back in the installer and verify that the case is correct for all entries on this page.

When you are done, click **Register**. CTE contacts the CipherTrust Manager and attempts to register the client with the specified options. The Register Host dialog box displays a message with the results of the registration request.
If the registration completed successfully, click **Finish**.

9. Restart the client to complete the installation process on the client.
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.

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

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

Using Ransomware

The following explains how using CipherTrust Transparent Encryption with Ransomware Protection can enhance the protection of your data:

Protect the File Server with both CipherTrust Transparent Encryption and Ransomware Protection

Use Ransomware Protection to improve data protection by encrypting sensitive data using CTE standard and LDT policies. Combining CTE encryption policies with Ransomware Protection strengthens your security posture. In this scenario, both CipherTrust Transparent Encryption and Ransomware Protection licenses are installed on the same server. All of the customer sensitive data is on this server. Data may be on a local drive, or on a CIFS/NAS share mounted on this server. Users are using a CTE policy to encrypt the data, provide CTE access control and protect the data from Ransomware Attacks. For this use case:

1. Install and register CipherTrust Transparent Encryption with Ransomware Protection.
2. Ensure RW license is available on CM.
3. Apply Ransomware Protection to the File Server volumes.
4. Encrypt sensitive data using CTE standard and LDT policies.
5. Ensure the policy is pushed by looking a the CipherTrust Manager GUI and ensuring that the GuardPoints display as Healthy and Green.

Using Ransomware Protection to protect End Points on Local and CIFS Shares

You can also protect endpoints with CipherTrust Transparent Encryption with Ransomware Protection. In this scenario, customer sensitive data is not on this endpoint but is being accessed using this endpoint. Data may be on an external share or NAS/CIFS share. User will only apply RW license on this end-point. CTE encryption and access control is not enforced on this server. An example of a use case for this scenario is when you have users with laptops who frequently use your network and access servers on it, but do not have any sensitive data locally on their laptops. A system like this might belong to a salesperson who travels and frequently uses other networks to access the internet. When they log on to your network, they access the sales network server and upload data to it. They could easily pick up a Ransomware Protection virus from another network. Using the CipherTrust Transparent Encryption Ransomware Protection solution would protect the data on their local volumes, mounted volumes, and the network servers they access from being infected with Ransomware Protection. For this use case:

1. Install and register CipherTrust Transparent Encryption with Ransomware Protection.
2. Ensure RW license is available on CM.
3. Apply Ransomware Protection to the File Server volumes.
4. Ensure the policy is pushed by looking a the CipherTrust Manager GUI and ensuring that the GuardPoints display as Healthy and Green.

Adding Trusted Processes in the Ransomware Protection policy

Users can create a white list of trusted processes and exclude these processes from RW monitoring. For example, you could set it so that a zip application zipping up files would not be flagged or blocked.

1. Use a User Set, and/or Process Set to control access by people, processes, etc.

2. Use a Ransomware Protection-exempted Process Set to exempt specific processes so that Ransomware Protection will not be enforced on the members of this process set.
3. Specify the process set to be excluded from monitoring, and the action taken on all other processes that attempt to access the sensitive data.

Note

- **Always** add your anti-virus software to your exemption list (process set). Ransomware Protection intermittently flags anti-virus software as ransomware and blocks it.
- If you use a TDE (Transparent Encryption software) other than CTE for any database encryption, then you must add the `database.exe` to the exemption list (process set). On initial encryption, SQL Server, for example, reads in all of the clear data and writes it back out as encrypted data, during Transparent Data Encryption (TDE). As such, it exhibits ransomware-like behavior and therefore, must be added to the CipherTrust Transparent Encryption Ransomware Protection exempted process list.

Creating GuardPoints for Ransomware Protection

Steps to create GuardPoints on individual clients and client groups are similar. GuardPoints can be created on the GuardPoints tab of individual clients and client groups.

Note

Using Ransomware Protection GuardPoints to protect Network Shares is compatible with CipherTrust Manager v2.14 and subsequent versions.

To create an RWP GuardPoint:

1. Open the **Transparent Encryption** application.

2. Select the client or client group on which you want to create a GuardPoint.
    - Click an RWP-enabled client under the **Client Name** column (**Clients** > **Clients**). These are the clients with RWP or CTE RWP as Protection Mode.
    - Click a client group under the **Client Group Name** column (**Clients** > **Client Groups**).

3. On the **GuardPoints** tab, click **Create GuardPoint**.
   When creating an **RWP** GuardPoint, (for volumes, without encryption) you do not need to specify a CTE policy. So, for clients with the RWP protection mode, the **Policy** field is unavailable.
   On clients with the **CTE RWP** protection mode, (for GuardPoint, with encryption), you can create RWP GuardPoints as well as other types of GuardPoints with policies. So, the **Policy** field is available for such clients. Although the field is available, do not select any policy when creating an RWP GuardPoint.
   Refer to Protection Modes for information on CTE protection modes.

4. (For clients with the **CTE RWP** protection mode) Select **Ransomware Protection** as the **Type** of device to protect. This is a mandatory field.
   For clients with the **RWP** protection mode, **Ransomware Protection** is the default **Type** and cannot be modified.

5. Specify the **Path** (volume or network share) to be protected. This is a mandatory field. Options to specify the GuardPoint paths are:
    - **Enter/Browse Path**: Select this option, and enter the volume path (for example, C:\, or D:\, or shared volume) by either typing or clicking the **Browse** button.

      Note

      - Ransomware Protection GuardPoints are applied at the volume level. Even if you specify the path of a folder or a file, the GuardPoint will be applied at the volume level.
      - If you specify a network share, *all the network shares to be mounted subsequently* will be protected.
      - A CTE client administrator can configure protection of all existing volumes and mount points, and those to be added to the client subsequently.
      - A maximum of 200 GuardPaths can be specified using the **Enter/Browse Path** option.

Browse Method

a. Click **Browse** to select the volume by browsing the client file system. This method prevents typographical errors and verifies client availability. This is the recommended method to specify individual paths.
   File system of a client that is not registered with the CipherTrust Manager cannot be browsed.

b. In the **Enter Path** field, specify the volume path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.

c. Click **Add**.

Manual Method

Alternatively, if you know the volume, manually enter volume in the given text box. Enter one volume per line.

- **Upload CSV**: Select this option and click **Browse** to upload the CSV file containing the list of one or more paths. This is the recommended method to specify a large number of paths in one step.

> **Note**
>
> If a manually entered path does not yet exist, check that you entered the path correctly. The CipherTrust Manager does not parse manually entered paths for correct syntax.

6. Click **Create**. A message appears prompting to confirm the reuse of these GuardPoint settings on another path.
    - Click **Yes** to use the same settings on another path. The Use Settings on Another Path dialog box is displayed. Perform the following steps:
        a. In the **Enter Path** field, specify the path. Alternatively, in the **Select Path** field, select the path from the on-screen file system browser, and click **Select Path**.
        b. Click **Add Path**. The newly added path appears under the Paths list on the left. Similarly, add as many paths as required.
        c. Click **OK**.
    - Click **No** if you do not want to use the same settings on another path.
7. Check the GuardPoint status, type:

```
secfsd -status guard
```

Setting Ransomware Protection Sensitivity

The sensitivity level determines how comprehensive the result list will be. The sensitivity level range is 1-10 where 1 is the **least** sensitive, so it allows more suspicious behavior to pass through. Conversely, 10 is the **most** sensitive, so it allows less suspicious behavior to pass through undetected.

There are three settings available for the sensitivity of the ransomware protection:

Monitor Mode

Monitoring mode generates a list of suspicious incidents. If you set the list to a low sensitivity level, more files will get encrypted before a given ransomware is detected. If you set it to a high sensitivity level, it may affect throughput and the list may contain more false positive results.

Sensitivity is set to a default of 8 at the time of installation because that score produces relatively few false hits. False hits look just like ransomware for brief moments. Increasing to a maximum of 10 should not produce results that are that different. You

can increase or decrease the sensitivity. If you see a lot of false positive results, decrease the sensitivity to eliminate them.

Block Mode

Block mode blocks the relevant suspicious behaviors. Sensitivity is also set to a default of 8 at the time of installation for Block mode. In Block mode, you can only increase the sensitivity.

Disable Mode

Disable mode disables Ransomware Protection for all GuardPoints on the clients linked with this profile. Therefore, it has nothing to log.

See Disabling Ransomware Protection for more information.

> **Note**
>
> Disable mode is **only** available with CipherTrust Manager v2.15 and subsequent versions.

Setting the Sensitivity Level

To adjust the sensitivity:

1. Initially, set the operation mode to **Monitor** when you create your Ransomware Protection profile.
2. Set the sensitivity level, type:

```
voradmin rwp sensitivity [1 through 10]
```

3. To check the sensitivity level, if it is not known, type:

```
voradmin rwp sensitivity get
```

4. After the list is generated, add the false positives entries to your process set to exempt them from future monitoring.
5. When false positives are no longer reported, set the operation mode to **Block** to block the relevant suspicious behaviors and maintain the sensitivity level.

Guarding Data on CIFS Servers and Clients

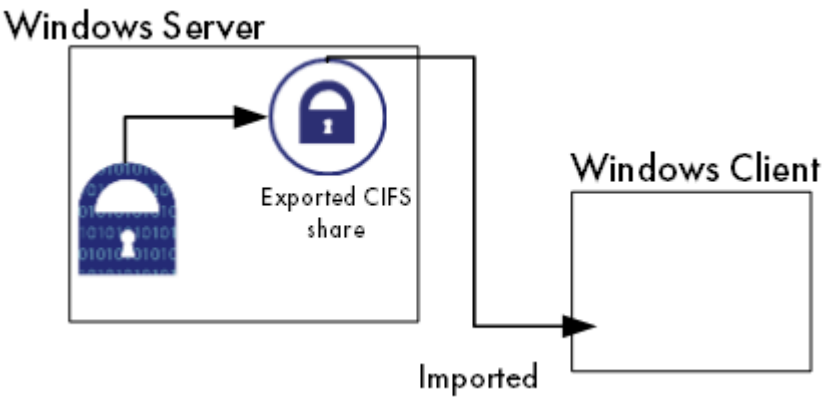
The Common Internet File System (CIFS) is a well-known and widely-deployed distributed file sharing protocol for Windows. *NIX (Unix/Linux-like operating systems) offer support, to share a directory with Windows, via SAMBA.

You can guard data on a CIFS share:

- On the Server side of the share (WIN and *NIX)
- On the client side (WIN client only)

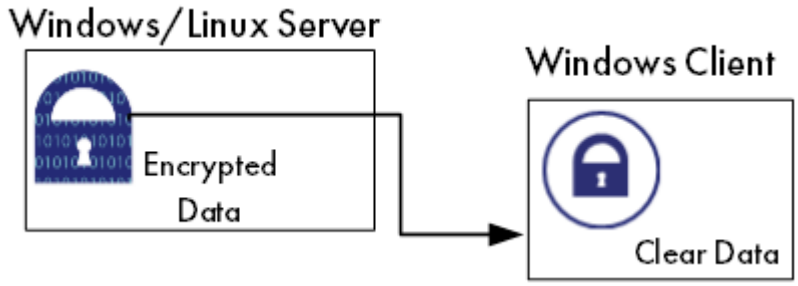
Guarding on the Windows SERVER side of a share

Guarding on the server side is supported for a directory. After which you can share the CIFS share out to another Windows server or client. **Do not** guard the share on the server side and then also on the client side. This will lead to double encryption and other problems.



Guarding on the Windows CLIENT side of a Share

You can guard on the client side, independent of the server side. The server side can be Windows or *NIX. For either the server or client side OS, the GuardPoint must be a File System that CipherTrust Transparent Encryption supports guarding, which is most typically a native FS.



PROS

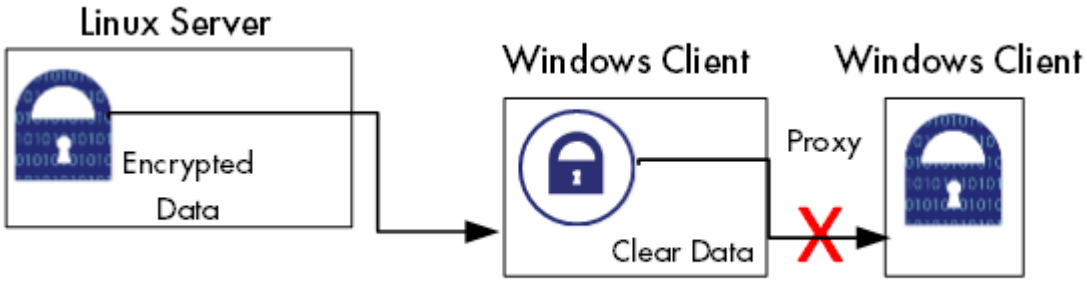
- Data sent over the channel is encrypted by the agent, above any channel protocol encryption.
- GuardPoint policy sees the processes on the host accessing files.

CONS

- More agents required, one per client, than guarding on the server side.

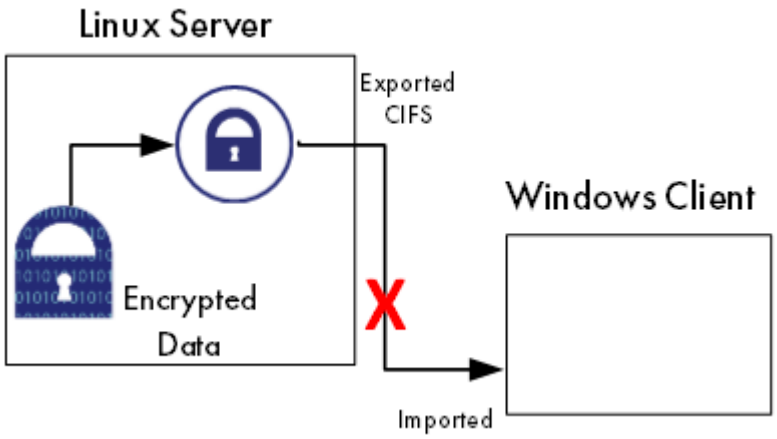
Proxy GuardPoint

Guarding on a client, and then exporting that client to another server, is not supported.



Guarding on the *NIX Server side of a Samba share

Guarding on a mounted CIFS/SAMBA share on *NIX is not supported. Use NFS to guard on the client side.



Whenever you are creating a GuardPoint on a CIFS share, you have two options.

1. Install CipherTrust Transparent Encryption agent on the CIFS server. Then create a GuardPoint on the network share. Have users connect remotely from their systems to the network share.
2. Install the CipherTrust Transparent Encryption agent on all remote user computers and again create a GuardPoint on the network share.

Note the following when creating a GuardPoint:

- When creating a GuardPoint, do not use the share mount point `'\share$. You must create the GuardPoint on a sub-folder of the mount point `\<serverName>\share$\folder1`
- In the policy, you must create a **UserSet** for remote users accessing the network share. This UserSet must be linked to the ProcessSet for `ntoskrn.exe` (Windows Only). Then grant the user Permit and Apply_key permissions.
- If a user that is logging in with `UserPrincipalName` (xyzuser@thales.com) is accessing the share folder, then the UserSet must contain the UPN. If the remote user logs on with a `sAMAccountName`(jharriman), then the UserSet must contain the sAMAccountName.

Special Cases for CTE Policies

This following section describes a CTE-specific configuration task related to configuring policies in the key manager.

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.

Security Rule Ordering for Polices

If you want to enforce restrictions when guarding NFS shares using an LDT or standard policy with a **CBC-CS1** key, note the following:

CipherTrust Transparent Encryption embeds and hides LDT and/or IV (initialization vector) attributes in the first 4K of files for NFS shares guarded with an LDT or standard policy with a **CBC-CS1** key. Embedding CipherTrust Transparent Encryption attributes increases the actual file size by 4K, and CTE hides that extra 4K when reporting the file size. The exception to this is when a backup/restore process reads/writes such files. This requires embedded attributes to be read/restored by the backup/restore process. In such cases, CipherTrust Transparent Encryption does not hide the 4K attribute space in the file. The backup user/process views the actual file size. Non-backup users/ applications view the file size as less than 4K.

If you want a security rule to enforce restricted access for reading file level attributes on such GuardPoints, you must specify the **Apply Key effect**. Alternatively, you can place the security rule that is enforcing the restricted access after the rule granting read/write access. This avoids application failure if the Apply key effect is not desired. For example, the order of the two rules in a policy that does not hide the user user-name would be:

- **Security Rule n**

Rule	Value
User	`<user-name>`
Action	Read-file-attribute and/or Read directory
Effect	permit

- **Security Rule n + 1**

Rule	Value
User	`<user-name>`
Action	all_ops
Effect	permit, apply-key

Assuming `<user-name>` is not affiliated with backup/restore operations, `<user-name>` would view the actual file size which is 4K larger than the size of the user data in the file. The returned file size can result in failure when user-name attempts to read/write files. By reordering rules n and n + 1, `<user-name>` will view the correct size hiding the 4K attribute space in the target file.

For more information, see Adding Security Rules in the CipherTrust Manager documentation.

Enhanced Encryption Mode

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

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

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.

Security Improvements

	AES-CBC	AES-CBC-CS1
Unique IV per-file	No	Yes
IV predictability	Yes	No

File System Support

	AES-CBC	AES-CBC-CS1
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 CipherTrust Manager, 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.

Note

- 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 CipherTrust Manager, 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 (initialization vector) 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 AES-CBC-CS1 key is supported on the 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.

Compatibility

	AES-CBC	AES-CBC-CS1
Local FS (Windows)	No change	Alternate Data Streams
NTFS file system	Supported	Supported
Azure File Share	Supported	**Not** supported with a standard policy on a system with a VMFILTR driver.

Note

AES-CBC-CS1 encrypted files on CTE Windows are not compatible with AES-CBC-CS1 encrypted files on CTE Linux. Do not create a policy on Linux that uses AES-CBC-CS1 keys if access to the same NFS GuardPoint is required by both Windows and Linux LAN clients.

Base IV file

To get the value of the base IV, type:

```
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.

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 CM

When you create a key in CTE, you enable Encryption Mode by selecting CTE Key Properties. See *Creating a New Key* in the Managing Policieschapter in the CTE Administrator Guide.

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 transformationor 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.

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 section:

- Agent Health Return Codes
- agentinfo (Java version)
- Backup
- voradmin secfs Commands
- vmsec
- vmutil

Agent Health Return Codes

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
SECFSD 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 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/secfs stop                //Linux

/etc/rc.d/rc2.d/S99secfs stop            //AIX
```

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

Note

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 GuardPoint/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
```

Backing up Databases after Encryption

After encrypting a database, CipherTrust Transparent Encryption cannot make a backup of the database. Both scheduled and manual backup fail. The problem was the user's policy. A policy used in this scenario must follow a few rules.

With a CBC_CS1 key, a guarded file is modified to have a 4096 byte header holding key information. When an **Apply Key** effect is specified, the CipherTrust Transparent Encryption code adjusts the length and file offset for this header. Without an **Apply Key** effect, the size and access of the offset include the CBC_CS1 header.

Thales recommends that you modify the first rule of your policy. Remove the action entry for `f_rd_att` from the first rule and add a new rule before it:

```
**action**: f_rd_att

**effect**: Permit, Apply Key
```

Policy processing starts with the first rule and continues until a matching rule is found. The effect for the matching rule is then applied.

For the `f_rd_att` action, this results in the secfs code including the CBC_CS1 key header and adjusts the file size value. Without the Apply Key effect, the file size includes the CBC_CS1 header size and the file appears as 4096 bytes larger than its real size.

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**

`Guardpoints`	Displays all the GuardPoints on the host.
`Policy`	Displays all the policies used on the host.

`logger`	Displays the logging details on the host.
`Status`	Displays the authentication settings on the host.

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

```
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:

```
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:

```
voradmin secfs status keys
```

Encryption keys are available

```
voradmin secfs status lock
```

FS Agent Lock: Disabled System Lock: Disabled

```
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

`check_install`	Verifies that the kernel component is running. This command checks CTE services and reports if any of the services are not running.
`challenge`	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.
`status`	Displays kernel configuration.
`vmdconfig`	Displays the vmd configuration.
`check_hwenc`	Determines whether this system supports hardware crypto.
`hwok`	Reports status of hardware signature.
`passwd [-p passwd]`	Enters the host password when the key manager is not network accessible. User can unlock the GuardPointswith this password.
`version`	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 CipherTrust Manager 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.

vmutil

Usage

```
vmutil <options> <operations>
```

Options

Option	Function	Description
-a	--agent	Specify agent type (vmd or pkcs11)
-d	--extdir	Specify location of external certificate and key set
-e	--error	Specify one or more errors for state report
-h	--help	Display help and exit
-l	--loglevel	Specify log output level (debug, info, warn, error or fatal)
-f	--force enabled	Force option for delete host operation
-v	--version	Display program version and exit

Operations

Operation	Description
certexpiry	Report the certificate expiration date for this agent
deletehost	Delete this client from the server
renewcerts	Renew certificate set for this agent
reportstate	Report agent state and error conditions to server
unregister	Unregister this agent/client from the server
updatecerts	Update external certificate and key set for this agent/client

Upgrading CTE on Windows

This chapter describes how to upgrade an existing VTE for Windows host to CipherTrust Transparent Encryption (CTE) for Windows and contains the following sections:

- Workaround for MSI CTE Typical, Silent, and Scheduled Upgrades
- Upgrading CTE Agents in an LDT Communication Group from 7.4.0 to 7.5.0 and post 7.5.0

Silent Upgrade

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 CipherTrust Manager that it is registered to or the upgrade will fail.

Upgrade using self-extracting .exe

```
vee-fs-7.3.0-135-win64.exe /s /v" /qn"
```

Upgrade using MSI

```
msiexec.exe /i vee-fs-7.3.0-135-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 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 CipherTrust Manager 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.

Prerequisites

The following prerequisites are mandatory for a successful upgrade of a CTE agent node:

1. Install all Microsoft update patches before scheduling a CTE Agent upgrade.
2. Make sure that your Windows version is Windows Server 2008 R2 and subsequent versions. The CTE scheduled upgrade feature is not compatible with previous versions.
3. For all types of upgrades, including interactive (GUI-based) and scheduled upgrades, the CTE client must be able to connect to the CipherTrust Manager to which it is registered.

4. When upgrading from a CipherTrust Transparent Encryption version that is prior to v7.1, you must **first** upgrade to v7.1 before scheduling an upgrade to subsequent versions from v7.1.

If you are upgrading CTE agents in an LDT Communication Group, the following prerequisites are also mandatory for a successful upgrade:

1. Disable the GuardPoints on the nodes to be upgraded:
    a. Go to the CipherTrust Manager UI.
    b. In the GuardPoint window, click the ellipsis on the right side of a GuardPoint and select disable to disable the GuardPoint.
    c. Repeat the steps for all of the GuardPoints on the nodes to be upgraded.
2. Stop CTE Services on the nodes to be upgraded:
    a. Go to **Control Panel > Services (local)**.
    b. Select **secfsd**.
    c. Select **Stop the Service**.

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>
UPGRADE_NO_CIFSGP=Yes
```

Note

You must set the `UPGRADE_NO_CIFSGP` variable to `yes` after ensuring that all CIFS GuardPoints are disabled. This is mandatory. The upgrade fails if any CIFS GuardPoints are enabled. The `UPGRADE_NO_CIFSGP` variable checks that LDT CIFS GuardPoints are disabled, or not present, in v7.5.0 and subsequent versions. For v7.4.0 and previous versions, it cannot verify the GuardPoint status.

Self-extracting .exe Example

```
 voradmin upgrade schedule C:\<Release.build-number>\vee-fs-7.3.0-135-win64.exe UPGRADE_NO_CIFSGP=Yes
```

Minor MSI Upgrades Only (Patches)

1. Before running `voradmin upgrade schedule`, check and remove any existing MSI packages from `C:\ProgramData\Vormetric`.
2. Type:

```
voradmin upgrade schedule C:\<Release.build-number>\vee-fs-7.3.0-158-win64.msi MINOR_UPGRADE=Yes REINSTALL=ALL REINSTALLMODE=vomus UPGRADE_NO_CIFSGP=Yes
```

System Response

```
    Creating and installing service to upgrade. CTE agent will be upgraded on next reboot.
```

Alternative MSI Method

1. Rename the package named: `vee-fs-7.3.0-158-win64.msi` to the previous install package name, ex: `vee-fs-7.3.0-135-win64.msi`
2. Type:

```
voradmin upgrade schedule C:\vee-fs-7.3.0-135-win64.msi REINSTALL=ALL REINSTALLMODE=vomus UPGRADE_NO_CIFSGP=Yes
```

Major MSI Installations

For a major MSI upgrade, the command is the same as that for the `. exe file`.

- Type:

```
voradmin upgrade schedule <CTE MSI installer path> UPGRADE_NO_CIFSGP=Yes
```

Example

```
    voradmin upgrade schedule C:\vee-fs-7.3.0-135-win64.msi
UPGRADE_NO_CIFSGP=Yes
```

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).

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-7.0.0.47-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-7.1.0.66-win64.msi
```

To upgrade successfully using MSI, you would need to rename the new installation binary to the previous file name of `vee-fs-7.0.0.47-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:

```
 (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.

Uninstalling CTE from Windows

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 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:

      ```
      msiexec.exe /x <Installation_executable> /qn` command.
      ```

    For example:

```
:::yaml
msiexec.exe /x vee-fs-7.3.0-135-win64.msi /qn
```

5. Reboot the system when prompted.
6. Remove the host record from the key manager.

Troubleshooting and Best Practices

Windows Systems

CTE will not register with the CipherTrust Manager

- If there is a firewall between the CipherTrust Manager and CTE, configure `vmd.exe` as a firewall exception on CipherTrust Manager for Windows. Otherwise, the CipherTrust Manager 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.

Support Contacts

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

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

Customer Support Portal

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

Tip

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

Telephone Support

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

Email Support

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