CipherTrust Transparent Encryption

CTE Agent for CipherTrust Manager

Windows Quick Start Guide

Release 7.2.0

Document Version 2

March 18, 2022

CTE Agent for CipherTrust Manager
7.2.0
March 18, 2022

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

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

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

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

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

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

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

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

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

Copyright © 2009-2022 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

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

Chapter 1: Overview of CTE

This document describes how to install CipherTrust Transparent Encryption (CTE) to protect data on physical or virtual machines.

CTE protects data at rest, residing on Direct Attached Storage (DAS), Network Attached Storage (NAS) or Storage Area Networks (SAN). This can be a mapped drive or mounted disk, as well as through Universal Naming Convention paths.

CTE secures data with little impact to application performance. It requires no changes to your existing infrastructure and supports separation of duties between data owners, system administrators, and security administrators.

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. **Note** This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". For example, the default installation directory is C:\Program Files\Vormetric\DataSecurityExpert\agent\. For example, the default installation directory is /opt/vormetric/DataSecurityExpert/agent/ for Linux and AIX, and C:\Program Files\Vormetric\DataSecurityExpert\agent\ for Windows.
CTE Agent	The software that you install on a physical or virtual machine in order to encrypt and protect the data on that machine. After you have installed the CTE Agent on the machine, you can use CTE to protect any number of devices or directories on that machine.
key manager	An appliance that stores and manages data encryption keys, data access policies, administrative domains, and administrator profiles
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.

Copyright © 2009-2022 Thales Group. All rights reserved.

- 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 or the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.
>
> All CTE documentation is available at https://thalesdocs.com/ctp/cte/index.html.

How to Protect Data with CTE

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

Policies specify:

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

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

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

Copyright © 2009-2022 Thales Group. All rights reserved.

Chapter 2: Configuring CTE for Windows with CipherTrust Manager

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

Installation Prerequisites

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

Network Setup Requirements

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

Communication through a Firewall

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

Browser Communications

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 for GuardPoints must have the following ports open:

- 7024
- 7025

Installing and Registering CTE

The Windows interactive install uses a standard InstallShield wizard that asks you a series of questions during the installation. After you install CTE, you are prompted to register it immediately with a key manager. CTE must be registered with a key manager before you can protect any of the devices on the host.

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

Copyright © 2009-2022 Thales Group. All rights reserved.

Prerequisites

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

- CipherTrust Manager installed and configured. See CipherTrust Manager Documentation for more information.
- 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 Groups for more information.

Procedure

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

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

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

8. On the *Ready to Install* page, click **Install**. When the installation is finished, the **Install Shield Wizard Completed** window opens.
9. On the *InstallShield Wizard Completed* page, make sure the **Register CipherTrust Transparent Encryption now** check box is selected and click **Finish**. The installer opens the Register Host wizard.

Copyright © 2009-2022 Thales Group. All rights reserved.

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

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

3. 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: <*hostName*>:<*port#*> . 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.

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

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

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

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

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

   WARNING

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

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

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

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

Copyright © 2009-2022 Thales Group. All rights reserved.

7. After the host has rebooted, you can verify the installation by checking CTE processes:
   a. In the system tray of the protected host, right-click the CipherTrust Lock icon.
   b. Select **Status**. Review the information in the **Status** window to confirm that the correct CTE version is installed and registered.
   - If you are using CipherTrust Manager version 2.2 or later, you can now use CipherTrust Manager to administer CTE on the client.

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

Guarding a Device with CipherTrust Manager

After you register a client with a CipherTrust Manager, you can create as many standard GuardPoints on the client as you need. These GuardPoints can protect an entire device or individual directories.

> **Note**
> For guarding using LDT on a local drive, or on a CIFS/Share drive, refer to the CTE-Live Data Transformation with CipherTrust Manager guide.

In order to guard a device or directory, you need to use the CipherTrust Manager Console to:

1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to use for the device or directory.
4. Assign a GuardPoint to the device or directory.

The following example creates a simple policy and uses it to guard a directory on a registered client. For all of the following procedures, you must be logged into the CipherTrust Manager Console as a CipherTrust Manager Administrator, and you must be in the domain with which the client is registered.

For details about any of these procedures or the options for domains, encryption keys, policies, and GuardPoints, see the CipherTrust Manager documentation.

Copyright © 2009-2022 Thales Group. All rights reserved.

Access the CipherTrust Manager Domain

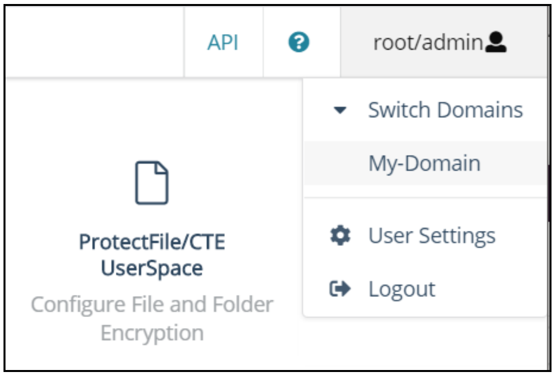
1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.

2. If the client you want to protect is registered to the default domain (root), proceed to "Create an Encryption Key" below. If you need to change to a different domain, do the following:

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

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

   c. The logged in user now shows the new domain name/user name.


API
root/admin
Switch Domains
My-Domain
User Settings
Logout
ProtectFile/CTE UserSpace
Configure File and Folder Encryption

Create an Encryption Key

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

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

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

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

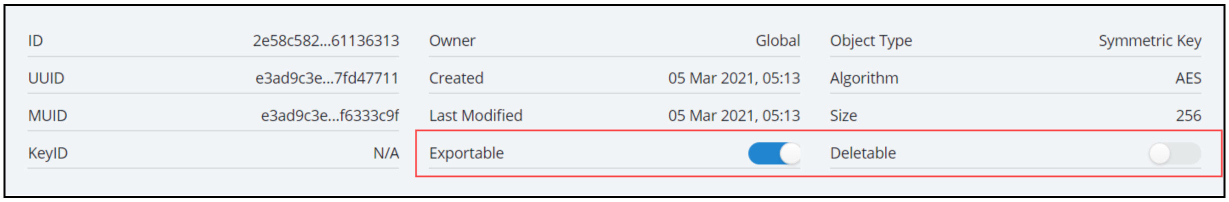
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.

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

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

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

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



ID	2e58c582...61136313	Owner	Global	Object Type	Symmetric Key
UUID	e3ad9c3e...7fd47711	Created	05 Mar 2021, 05:13	Algorithm	AES
MUID	e3ad9c3e...f6333c9f	Last Modified	05 Mar 2021, 05:13	Size	256
KeyID	N/A	Exportable	●	Deletable	○

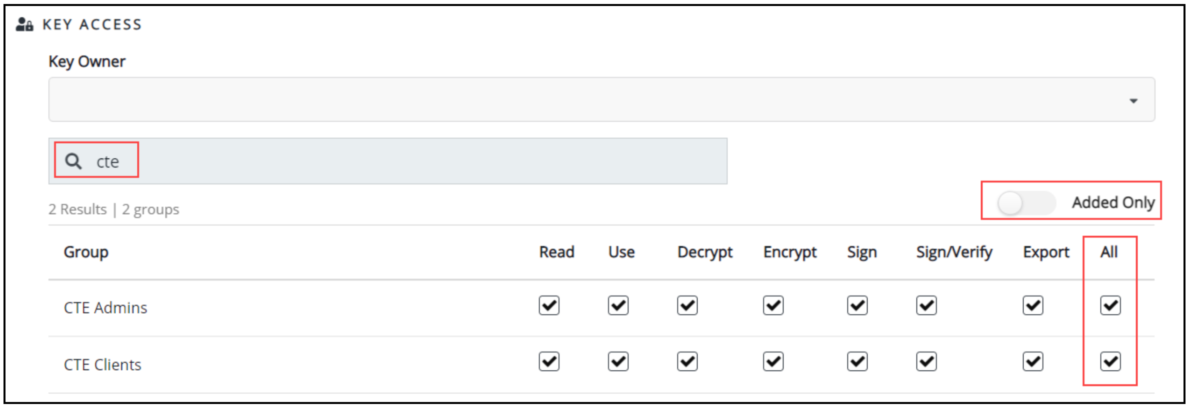
Copyright © 2009-2022 Thales Group. All rights reserved.

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

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

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

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



KEY ACCESS

Key Owner

cte

2 Results | 2 groups

○ Added Only

Group	Read	Use	Decrypt	Encrypt	Sign	Sign/Verify	Export	All
CTE Admins	☑	☑	☑	☑	☑	☑	☑	☑
CTE Clients	☑	☑	☑	☑	☑	☑	☑	☑

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

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

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

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

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

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

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

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

     - CBC
     - CBC CS1
     - XTS

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

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

Create a Standard Policy

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

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

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

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

Copyright © 2009-2022 Thales Group. All rights reserved.

Field	Description
Name	A unique name for the policy. Make sure you use a name that is descriptive and easy to remember so that you can find it quickly when you want to associate it with a GuardPoint. This example uses "Simple-Policy".
Policy Type	The type of policy you want to create. In this example, we will create a **Standard** policy.
Description	A user-defined description to help you identify the policy later. For example: Standard policy for new GuardPoints
Learn Mode	Learn Mode provides a temporary method for disabling the blocking behavior of CTE/CTE-LDT policies. While useful for quality assurance, troubleshooting, and mitigating deployment risk, Learn Mode is not intended to be enabled permanently for a policy in production. This prevents the policy Deny rules from functioning as designed in the policy rule set. Ensure that the policy is properly configured for use in Learn Mode. Any Security Rule that contains a Deny effect must have Apply Key applied as well. This is to prevent data from being written in mixed states, resulting in the loss of access or data corruption. Apply Key will have no effect when combined with a Deny rule unless the policy is in Learn Mode.
Data Transformation	If you select **Standard** as the policy type, also select the the **Data Transformation** option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

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

5. On the Security Rules page, define the security rules that you want to use.

   CipherTrust Manager automatically adds a default security access rule with an action of `key_op` and the effects `Permit` and `Apply Key`. This rule permits key operations on all resources, without denying user or application access to resources. This allows it to perform a rekey operation whenever the encryption key rotates to a new version.

   To add additional security rules, click **Create Security Rule** and enter the requested information. For details about adding security rules, see the CipherTrust Manager documentation.

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

Copyright © 2009-2022 Thales Group. All rights reserved.

6. On the Create Key Rule page, click **Create Key Rule** and enter the following information:

Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Current Key Name	Click **Select** to choose an existing key or create a new one. If the data has not yet been encrypted, select **clear_key**. Otherwise select the name of the non-versioned key that is currently being used to encrypt the data. In this example, select **clear_key**.
Transformation Key Name	Click **Select** to choose an existing versioned key or to create a new one. CTE uses the versioned key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the **Current Key Name** field and re-encrypts it using the key specified in this field.

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

7. On the Data Transformation page, click **Create Data Transformation Rule** and enter the following information:

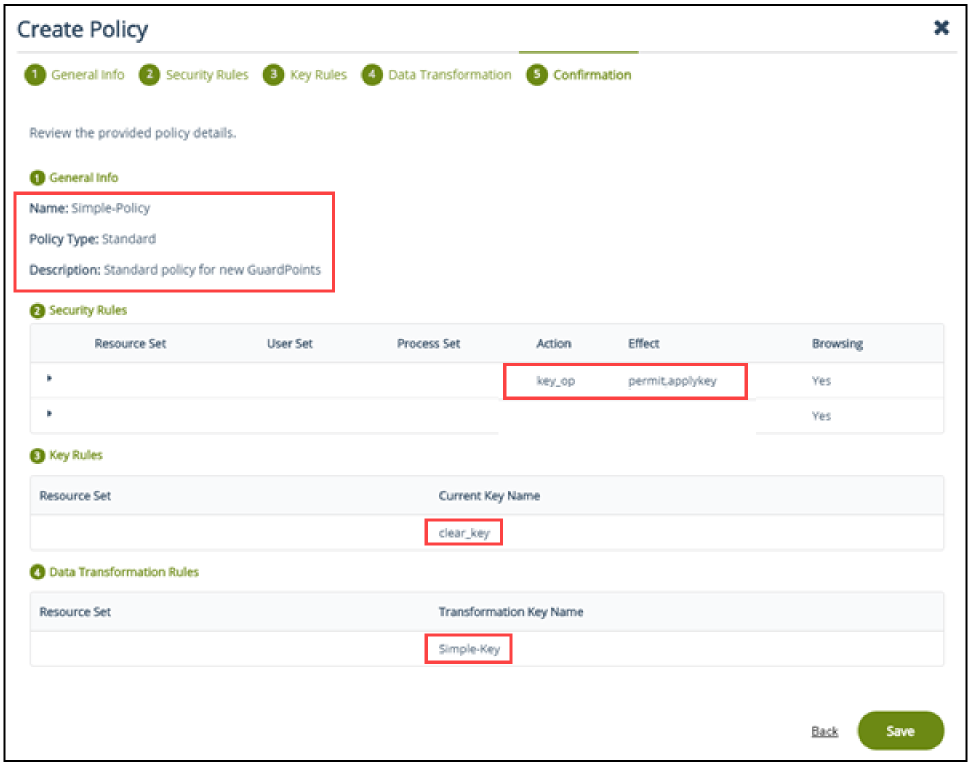
Field	Description
Resource Set	If you want to select a resource set for this key rule, click Select and either choose an existing resource set or create a new one. Resource sets let you specify which directories or files will either be encrypted with the key or will be excluded from encryption with this key.
Transformation Key Name	Click **Select** to choose an existing key or to create a new one. CTE uses the key specified in this field to encrypt the data in the GuardPoint. If the data is currently encrypted, CTE decrypts it using the key specified in the **Current Key Name** field and re-encrypts it using the key specified in this field. For this example, select the key Simple-Key you created in "Create an Encryption Key" on page viii.

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

8. Click **Next**.

Copyright © 2009-2022 Thales Group. All rights reserved.

9. On the confirmation page, review the information for the policy and click **Save**.



Create Policy

Review the provided policy details.

1 General Info

Name: Simple-Policy

Policy Type: Standard

Description: Standard policy for new GuardPoints

2 Security Rules

	Resource Set	User Set	Process Set	Action	Effect	Browsing
▸				key_op	permit,applykey	Yes
▸						Yes

3 Key Rules

Resource Set	Current Key Name
	clear_key

4 Data Transformation Rules

Resource Set	Transformation Key Name
	Simple-Key

Create a GuardPoint

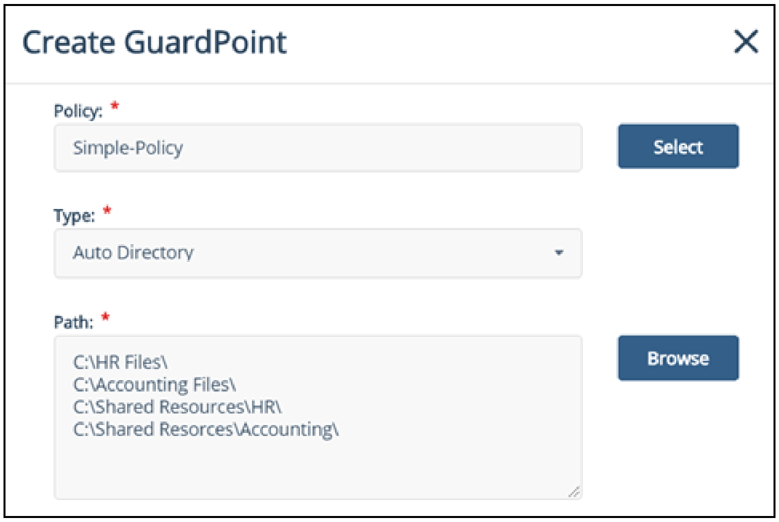
1. Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
   - `C:\HR Files\`
   - `C:\Accounting Files\`
   - `C:\Shared Resources\HR\`
   - `C:\Shared Resorces\Accounting\`

   > **Tip:** If you want to encrypt data without taking the device offline, you must use CipherTrust Transparent Encryption - Live Data Transformation.

2. In the Applications page of the CipherTrust Manager Console, select the **CTE** application.
3. In the Clients table, click on the name of the client you want to protect.
4. Above the GuardPoints table, click **Create GuardPoint**.
5. In the Create GuardPoint page:
   a. In the **Policy** field, select the policy you created earlier.
   b. In the Type field, select the type of device. You can guard a directory or a raw/block device. For this example, select **Auto Directory**.
   c. In the **Path** field, enter the directories you want to protect with this policy or click **Browse** to select them from a explorer window.

      If you want to enter multiple paths, put each path on its own line. For example:

Copyright © 2009-2022 Thales Group. All rights reserved.



Create GuardPoint

Policy: * Simple-Policy

Type: * Auto Directory

Path: *
C:\HR Files\
C:\Accounting Files\
C:\Shared Resources\HR\
C:\Shared Resorces\Accounting\

d. Click **Create**.

e. If you want to use the same policy and GuardPoint type on another path, click **Yes** when prompted. Otherwise, click **No**. For this example, click No.

The CTE clients pull the GuardPoint configuration information from the CipherTrust Manager.

6. Type the following to transform the data:

```
# dataxform --rekey --print_stat --preserve_modified_time --gp <pathToGP>
```

When the data transformation has finished, applications can resume accessing the now-protected data. (See the “*CTE Data Transformation Guide”* for more information.)

Copyright © 2009-2022 Thales Group. All rights reserved.