THALES

CipherTrust Transparent Encryption

CTE Agent for CipherTrust Manager

Linux Quick Start Guide

Release 7.2.0

Document Version 3

April 11, 2022

CTE Agent for CipherTrust Manager
7.2.0
April 11, 2022

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.

Contents

Preface

Audience

The *CTE Agent for CipherTrust Manager* is intended for system administrators who install and configure CipherTrust Transparent Encryption (CTE) on Linux.

The CTE Agent Documentation Set

The following guides are available for CTE Agent:

- *CTE Agent for Linux Quick Start Guide*
- *CTE Agent for Linux Advanced Configuration and Integration Guide*
- *CTE Agent for Windows Quick Start Guide*
- *CTE Agent for Windows Advanced Configuration and Integration Guide*
- *CTE Agent for AIX Installation and Configuration Guide*
- *CTE Data Transformation Guide*
- *CTE-Live Data Transformation with Data Security Manager*
- *CTE-Live Data Transformation with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent with Data Security Manager*
- *Compatibility Matrix for CTE Agent for AIX with CipherTrust Manager*
- *Compatibility Matrix for CTE Agent for AIX with Data Security Manager*
- *Release Notes for CTE for Linux Version 7.2.0.128*
- *Release Notes for CTE for Windows Version 7.2.0.128*
- *Release Notes for CTE for AIX Version 7.2.0.56*

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

Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

Table 2-1: Typographical Conventions

Convention	Usage	Example
bold regular font	GUI labels and options	Click the **System** tab and select **General Preferences**.

Table 2-1: Typographical Conventions (continued)

Convention	Usage	Example
bold italic monospaced font	Variables or text to be replaced	https://<***Token Server name***>/admin/ Enter password: <***Password***>
`regular monospacedfont`	• Commands and code examples • XML examples	`session start iptarget=192.168.253.102`
italic regular font	GUI dialog box titles	The *General Preferences* window opens.
	File names, paths, and directories	*/usr/bin/*
	Emphasis	*Do not* resize the page.
	New terminology	*Key Management Interoperability Protocol (KMIP)*
	Document titles	See *CTE Agent for CipherTrust Manager* for information about CipherTrust Transparent Encryption.
quotes	• File extensions • Attribute values • Terms used in special senses	".js", ".ext" "true" "false", "0" "1+1" hot standby failover

Notes, Tips, Cautions, and Warnings

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

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

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

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

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

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

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

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

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

Sales and Support

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

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

For support and troubleshooting issues:

- https://supportportal.thalesgroup.com
- (800) 545-6608

For Thales Sales:

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

Chapter 1: Overview of CTE

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

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

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

CTE Terminology

The CTE documentation set uses the following terminology:

Term	Description
CTE	CipherTrust Transparent Encryption is a suite of products that allow you to encrypt and guard your data. The main software component of CTE is the CTE Agent, which must be installed on every host whose devices you want to protect. **Note** This suite was originally called Vormetric Transparent Encryption (VTE), and some of the names in the suite still use "Vormetric". For example, the default installation directory is /opt/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.

- 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.

Chapter 2: Configuring CTE for Linux with CipherTrust Manager

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

Installation Prerequisites

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

Recommendations and Considerations

- The host on which you want to install CTE *must* support AES-NI hardware encryption. If it does not, any attempt to install or upgrade CTE to release 7.0.0 or later will fail.
- Thales recommends that you install CTE in the default location.
- Make the installation root directory `/opt` a real directory. If `/opt` is a symlink, you **must** use the `-d` option to specify the installation directory, which must be a real directory.

  For example:

  ```
  # ./vee-fs-7.2.0-128-rh8-x86_64.bin -d /home/hello/
  ```

- Ensure read/write permission is granted to other users accessing your shared resource.

Network Setup Requirements

- IP addresses, routing configurations and DNS addresses must allow 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 host is a virtual machine, the VM must be deployed and running.

Port Configuration Requirements

(missing or bad snippet)

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 for GuardPoints must have the following ports open:

- 7024
- 7025

Installing and Registering CTE

Thales provides a standard interactive installation script that asks you a series of questions during the install. The script prompts you to register CTE with a key manager immediately after the installation has finished. CTE must be registered with a key manager before you can protect any of the devices on the host.

> **Note**
> Do not install CTE on network-mounted volumes like NFS.

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 where you will install the CTE Agent as `root`. You cannot install the CTE Agent without `root` access.
2. Copy or mount the installation file to the host system. If necessary, make the file executable with the `chmod` command.
3. Install the CTE Agent. A typical installation uses the following syntax:

   ```
   # ./vee-fs-<release>-<build>-<system>.bin
   ```

   For example:

   ```
   # ./vee-fs-7.2.0-128-rh8-x86_64.bin
   ```

   To install the CTE Agent in a custom directory, use the `-d <custom-dir>` option. For example:

   ```
   # ./vee-fs-7.2.0-128-rh8-x86_64.bin -d /home/my-cte-dir/
   ```

   > **Note:** If possible, Thales recommends that you use the default directory `/opt/vormetric`.

   To view all installer options, use the `-h` parameter. For example:

   ```
   # ./vee-fs-7.2.0-128-rh8-x86_64.bin -h
   ```

4. The Thales License Agreement displays. When prompted, type **Y** and press Enter to accept.

   The install script installs the CTE Agent software in either `/opt/vormetric` or your custom installation directory and then prompts you about registering the CTE Agent with a key manager.

```
Welcome to the CipherTrust Transparent Encryption File System Agent
Registration Program.

Agent Type: CipherTrust Transparent Encryption File System Agent
Agent Version: 7.2.0.129


In order to register with a CipherTrust Manager you need a valid registration
token from the CM.

Do you want to continue with agent registration? (Y/N) [Y]:
```

5. Enter **Y** to continue with the registration process. The install script prompts you to enter the host name or IP address of the CipherTrust Manager with which you want to register CTE.

   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:

```
Do you want to continue with agent registration? (Y/N) [Y]: Y

Please enter the primary key manager host name: 10.3.200.141:8445

You entered the host name 10.3.200.141
Is this host name correct? (Y/N) [Y]: Y
```

6. Enter the client host name when prompted.

```
Please enter the host name of this machine, or select from the following
list.

[1] sys31186.qa.com
[2] 10.3.31.186

Enter a number, or type a different host name or IP address in manually:
What is the name of this machine? [1]: 2
You selected "10.3.31.186".
```

7. Enter the CipherTrust Manager registration token, profile name, host group and host description. If you omit the profile name, CipherTrust Manager associates the default client profile with this client.

```
Please enter the registration token: 12345
Please enter the profile name for this host: My-Profile
Please enter the host group name for this host, if any:
Please enter a description for this host: West Coast Datacenter server 5

Token            : 12345
Profile name     : My-Profile
Host Group       : (none)
Host description : West Coast Datacenter server 5
Are the above values correct?  (Y/N) [Y]: Y
```

8. At the hardware association prompt, select whether you want to enable the hardware association feature to prevent cloned machines from accessing the key manager. The default is **Y** (enabled):

```
It is possible to associate this installation with the hardware of this
machine.  If selected, the agent will not contact the key manager or use any
cryptographic keys if any of this machine's hardware is changed.  This
can be rectified by running this registration program again.
Do you want to enable this functionality?  (Y/N) [Y]: Y
```

9. At the LDT prompt, specify whether you want this client to use CipherTrust Transparent Encryption - Live Data Transformation (CTE-LDT).

```
Do you want this host to have LDT support enabled on the server? (Y/N) [N]: Y
```

10. If you are planning to create GuardPoints on NFS shares, enter the name of the LDT Communication Group that this node will join.

```
Enter the LDT Communication Group name: LCG1
```

> **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.**

11. At the Cloud Object Storage (COS) prompt, specify whether you want this client to use CTE COS.

```
Do you want to configure this host for Cloud Object Storage? (Y/N) [N]:
```

12. > **Note:** You can only install the Cloud Object Storage feature during CTE installation. You cannot install it post installation.

13. CTE finishes the installation and registration process.

```
Generating key pair for the kernel component...done.
Extracting SECFS key
Generating EC certificate signing request for the vmd...done.
Signing certificate...done.
Enrolling agent with service on 10.3.200.141...done.
Successfully registered the CipherTrust Transparent Encryption File System Agent
with the
CipherTrust Manager on 10.3.200.141.

Installation success.
```

14. 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:

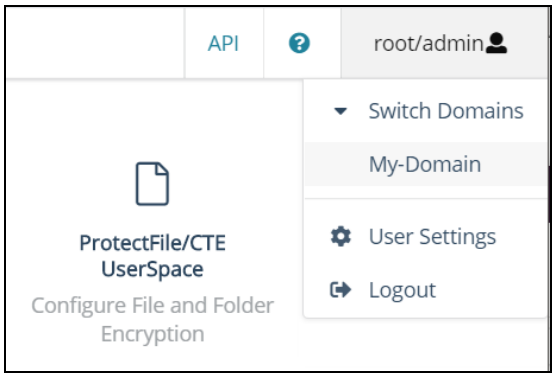
1. Access the CipherTrust Manager domain in which the client is registered.
2. Identify or create an encryption key that CTE will use to encrypt the data on the device or directory.
3. Identify or create a policy for the device or directory that specifies the access controls and the encryption keys to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

Access the CipherTrust Manager Domain

1. In a web browser, navigate to the URL of the CipherTrust Manager Console you want to use and log in with CipherTrust Manager Administrator credentials.
2. If the client you want to protect is registered to the default domain (root), proceed to "Create an Encryption Key" below. If you need to change to a different domain, do the following:
   a. In the top menu bar, click the user name **root/admin** on the right-hand side.
   b. Select **Switch Domains**, then select the domain in which the client is registered.
   c. The logged in user now shows the new domain name/user name.



Create an Encryption Key

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

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

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

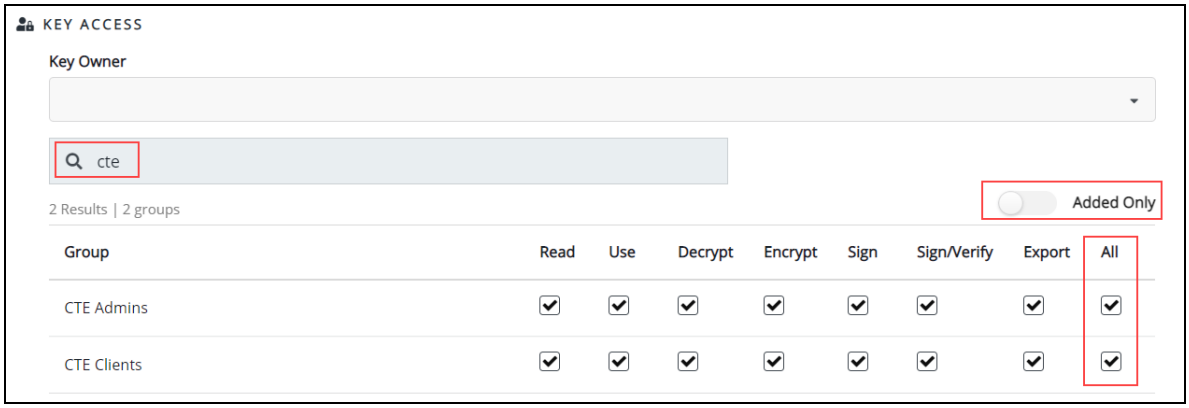
2. Above the Key table, click **Create a New Key**.
3. In the **Key Name** field, add a name for the key. This name must be unique. For example, Simple-Key.
4. In the **Key Usage** section, make sure **Encrypt** and **Decrypt** are selected.
5. Click **Create**. CipherTrust Manager displays the properties for the new key.
6. In the general options area, enable the **Exportable** option.

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

7. In the **Key Access** section, do the following:
   a. In the Search Groups box, type "cte".

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

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



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

8. Click the **CTE** tab and set the following properties:
   - **CTE Versioned**: Specify whether the key is versioned. By default, the key is set as versioned.

     For a standard policy, you should clear this check box. If you do not, the key will *not* appear in the keys list when you add the key rule to the standard policy.
   - **Persistent on Client**: Specify whether the key is stored in persistent memory on the client.

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

     When the check box is left clear, the key is downloaded to non-persistent memory on the client. Every time the key is needed, the client retrieves it from the CipherTrust Manager. This is the default setting.
   - **Encryption Mode**: Encryption mode of the key. The options are:
     - CBC
     - CBC CS1
     - XTS

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

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

Create a Standard Policy

1. In the Applications page of the CipherTrust Manager Console, select the **Transparent Encryption** application.
2. In the sidebar on the Clients page, click **Policies**.
3. Click **Create Policy**. CipherTrust Manager displays the Create Policy Wizard.
4. On the General Info page, set the following options:

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

Field	Description
Data Transformation	If you select **Standard** as the policy type, also select the the **Data Transformation** option to tell CTE that you want to change the current encryption key used on the data in the GuardPoint, or that you want to encrypt clear-text data for the first time. This option is only displayed for Standard policies.

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

5. On the Security Rules page, define the security rules 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**.

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.

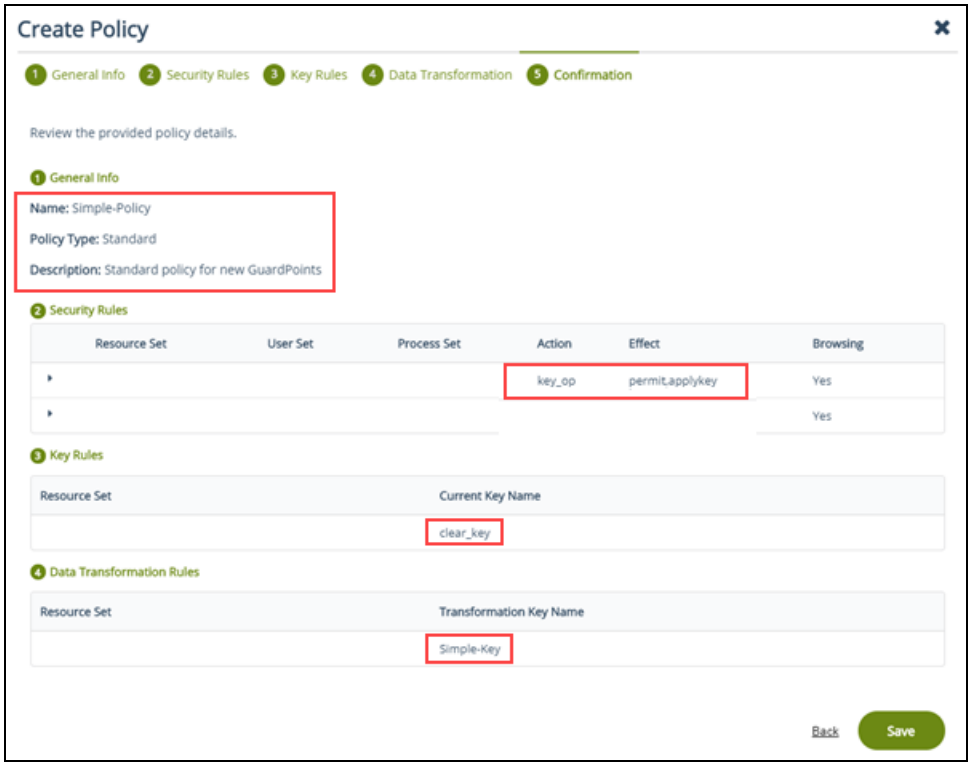
When you are done, click **Next**.

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 7.

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

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



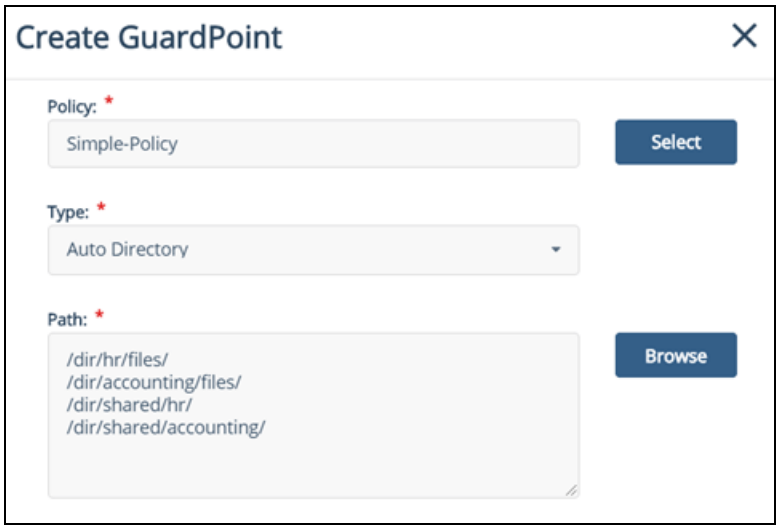
Create a GuardPoint

1. Stop all applications that are accessing the device you want to protect. In this example, we are going to protect the following directories with the same policy and encryption key:
   - /dir/hr/files
   - /dir/accounting/files
   - /dir/shared/hr
   - /dir/shared/accounting

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

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

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



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

   The 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.)