CipherTrust Transparent Encryption (CTE) for Windows

Release Notes

- **Release: 7.0.0.47**
- **Date: September 22, 2020**

New Features and Enhancements

Release 7.0.0.47 of CipherTrust Transparent Encryption (CTE) for Windows fixes known defects and addresses known vulnerabilities.

The major improvements to CTE for Windows in this release are:

- Enhancements to CTE-Efficient Storage:
  - Rekey is now available for ES GuardPoints on Windows.
  - Full device protection is now supported, and a new use case describing its use has been added to the documentation.
  - You can now add ES GuardPoints to clustered ES devices.

  For details about these enhancements, see the CTE-Efficient Storage chapter in the *CTE Agent for Windows Advanced Configuration and Integration Guide*.
- Improvements to the lazy transformation process. In previous releases, when CTE detected that a file had changed, it would re-scan the entire GuardPoint. Now CTE just transforms the changed file and does not perform a re-scan on the GuardPoint.
- CTE for Windows has made the following improvements to CTE-Live Data Transformation (CTE-LDT):
  - When CTE-LDT is suspended, CTE no longer creates the LDT metadata for each file.
  - After CTE performs the initial scan of the GuardPoint, it displays a message saying how much space will be required for CTE-LDT metadata.

Name Change to CipherTrust Transparent Encryption

Vormetric Transparent Encryption (VTE) is now called CipherTrust Transparent Encryption (CTE).

> **Note**
> Some of the names in the CTE suite still use "Vormetric".
>
> For example, the default installation directory is `C:\Program Files\Vormetric\DataSecurityExpert\agent\`.

CTE and CipherTrust Manager Integration

Thales now offers two key managers that work with CTE:

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

Both key managers can be set up as either a security-hardened physical appliance or a virtual appliance, and both provide access to the protected hosts through a browser-based, graphical user interface as well as an API and a CLI. Thales recommends that you use the CipherTrust Manager unless you need a feature that is only supported by the DSM, as described below.

The CipherTrust Manager currently supports all CTE for Windows features *except* for CTE-Efficient Storage. (For details about CTE-Efficient Storage, see the *CTE Agent for Windows Advanced Configuration and Integration Guide*.)

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

> **Note**
> For a list of CTE versions and supported operating systems, see the *Compatibility Matrix for CTE Agent with CipherTrust Manager* and the *Compatibility Matrix for CTE Agent with Data Security Manager*.

Upgrading Existing VTE Hosts to CTE 7.0.0.47

Currently, you can only upgrade a VTE for Windows host to CTE version 7.0.0.47 if you continue to use the DSM as your key manager. You cannot upgrade a VTE host to CTE and then register the upgraded CTE host with CipherTrust Manager. The migration path to CipherTrust Manager will be available in a future release.

CTE Documentation Set

The CTE Documentation Set has been expanded to include CipherTrust Manager and reorganized to make the information easier for customers to navigate. The CTE documentation set in version 7.0.0 includes the following books:

- *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-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 7.0.0.47*
- *Release Notes for CTE for Windows Version 7.0.0.47*
- *Release Notes for CTE for AIX Version 7.0.0.11*

Resolved Issues

- **AGT-29013 [CS0996844]: Windows 2012 (non-R2) failed to boot up after uninstalling VTE 6.3.1.43**

  For some versions of VTE 6.3.1, if you uninstall the VTE Agent on a Windows 2012 server, the VTE Agent is unable to cleanly remove its installed driver entries from the Windows registry. These leftover registry entries cause the Windows 2012 server to crash on boot. This issue has only been observed on Windows 2012.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-28677 — Lazy rekey triggers incorrectly due to alternate data stream access**

  Some applications create alternate data streams (ADS) associated with files that store application and/or user defined data. For some versions of VTE 6.3.1, when one of these data streams was accessed by an application, the LDT process was incorrectly rescanning the GuardPoint looking for a rekey event.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-27717 [CS0971454] — Files show half encrypted and half in clear**

  For some versions of VTE 6.3.1, there is an interoperability issue between VTE LDT and Sophos AV.

  When the LDT process begins transforming a file, Sophos AV starts scanning the file. LDT opens the file without caching, but Sophos AV start scanning the file with caching enabled.

  This discrepancy caused the VTE driver to return encrypted data and dirty the cache.

  This issue has been fixed in this release of the CTE Agent.

- **AGT-28420/AGT-27854 [CS0982045] — Servers reboot continuously after an LDT policy is applied to the GuardPoint**

  For some versions of VTE 6.3.1, the Windows CTE Agent is crashing on specific physical systems because of the new Kernel Key Protection Feature. This issue is reproducible only on physical systems.

  This issue has been fixed in this release of the CTE Agent.

Known Issues

- **AGT-29799 — Object Set not defined error displays incorrectly after applying an In-place Data Transformation - Device policy to a GuardPoint**

  If you apply an In-place Data Transformation - Device policy to a GuardPoint, the CTE Agent incorrectly logs the messages `[SecFS, 0] PID[pid] Object Set (_empty-0_) not defined` and `[SecFS, 0] PID[pid] Object Set (_empty-0_) used but not defined`. These messages can be safely ignored.

- **AGT-29791 — LDT data corruption issues after upgrading to 7.0.0 and restoring GuardPoint files from backup with Microsoft Defender**

  If you are running Microsoft Defender on a host with LDT GuardPoints, you must disable Microsoft Defender's On Access Scanning while restoring encrypted LDT GuardPoints.

  When the data in an encrypted LDT GuardPoint is backed up, the back up information also includes the LDT metadata, which includes the encryption type and the key used to encrypt the file. When the encrypted data is restored in the GuardPoint, the metadata for each file is restored along with the file.

  If Microsoft Defender On Access Scanning is running during the restore procedure, it may attempt to read the file before the file and its metadata are fully restored. When Microsoft Defender requests access from the CTE Agent, the CTE Agent may not be able to find the correct key and the decryption of the file will fail. This also corrupts the system cache with encrypted data.

  Workaround

  To work around this issue, you can do one of the following:

  - Disable Microsoft Defender's On Access Scanning until the LDT GuardPoint has been fully restored.
  - Reboot the system after the LDT GuardPoint has been fully restored to clear the system cache.

- **AGT-29611 — system crashed while checking voradmin esg status**

  If you run the `voradmin esg status` command immediately after guarding a CTE-Efficient Storage device or rekeying an ES GuardPoint, the system may crash if the CTE-Efficient Storage process has not yet finished setting up the internal memory structures it needs to intialize or rekey the GuardPoint.

  Workaround

  Always wait for a few minutes before running the `voradmin esg status` command after initializing or rekeying a GuardPoint.

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/
- CPL_Sales_AMS_TG@thalesgroup.com
- (888) 267-3732

Notices and License

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.