# CipherTrust Transparent Encryption (CTE) for Windows

## Release Notes

- **Release: 7.1.1.30**
- **Date: July 08, 2021**

## New Features and Enhancements

Release 7.1.1.30 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:

## CTE

- **SharePoint 2019**

  Support added for SharePoint 2019

- **Export to CSV**

  Support output of voradmin command into a CSV file: `voradmin ldt report <guard path> <log file>`

- **DSM to CM communication**

  Enhance CTE Challenge/ Response to return an error after wait timeout with DSM, CipherTrust Manager communication

- **Anti-virus support**

  Support for Sentinel One AV

## CipherTrust Intelligent Remediation

CipherTrust Intelligent Remediation enables organizations to assess all of their data, discover and protect sensitive data, and classify data according to various data privacy laws, by using the CipherTrust Intelligent Remediation solution with CipherTrust Data Discovery and Classification for finding and classifying sensitive data, and CipherTrust Transparent Encryption for encrypting that data. This protects customer data, achieves compliance, and best practice requirements. It helps a company avoid devastating financial, legal and reputational consequences that can occur if an organization's network is breached and sensitive data is stolen.


Copyright © 2009-2021 Thales Group. All rights reserved.

# Documentation Enhancements

- All CTE documentation is available at https://thalesdocs.com/ctp/cte/index.html.
- The CTE Compatibility Portal is now online.

> **Note:** The portal works best with Firefox and Chrome.

# Resolved Issues

- **AGT-31757 [CS1035960]: When LDT policy is applied on a GuardPoint, user is unable to delete a GuardPoint subdirectory**

  A race condition prevented the LDT process from reading the GuardPoint metadata. This then prevented the renaming of directories within the GuardPoint. This issue has been fixed.

- **AGT-31806 [CS1038224]: VTE Agent not validating the DSM certificate**

  Due to an error in the runtime engine used to perform encrypted communications with the server, certificate peer verification was inadvertently disabled, resulting in this vulnerability. That error is corrected with this fix.

- **AGT-33471 [CS1060166]: Windows Server with CTE agent may crash with extremely long file/path names**

  CTE has been changed to accommodate the number of characters.

- **AGT-33682 [CS1060061]: CTE Agent unable to report the correct agent health status**

  Occasionally, CTE kernel agent was unable to access the status file because of a sharing violation.This has been fixed.

- **AGT-33928 [CS1045438]: Windows Server with CTE Agent may crash when the source and destination file names are the same during the rename process**

  This has been fixed.

# Known Issues

## CTE

- **AGT-26477: When the ESG Data transformation is in progress, and Disk Manager is open, Disk manager does not refresh automatically**

  **Workaround:** Close the Disk Manager and manually reopen it, or click **Action > Refresh**.

- **AGT-31170: Incompatibility issue between McAfee AV and CTE Agent**

  If you install the CTE Agent before you install McAfee VirusScan Enterprise + Antispyware Enterprise 8.8, McAfee may not initialize or be able to scan the host.

  **Workaround:** Install McAfee before installing the CTE Agent.

- **AGT-31324: When LDT policy is applied on a CIFS share, exclusively open files will be skipped from rekey**

  If the files are opened exclusively by an application, the LDT process cannot open these files and skips them.

  **Workaround:** Stop the application accessing the files so it can release the reference to the files. After the application releases the reference to the file, LDT can finish the transformation.


Copyright © 2009-2021 Thales Group. All rights reserved.

- **AGT-31760: Disk management takes a long time to open after installing CTE**

  If MPIO is configured on the host, disk management may take a long time to open after you install the CTE Agent. This issue resolves itself after the host reboots.

  **Workaround:** Reboot the host.

## LDT

- **AGT-32498: On Windows 2019 DFSR node, LDT status may display as INCOMPLETE**

  On a Windows 2019 DFSR configuration, when LDT policy is applied to a GuardPoint, LDT may temporarily transistion into an Incomplete state. LDT will start again and complete the rekey.

## CipherTrust Intelligent Remediation

- **Changing PQS Schema**

  Thales does not support changing schemas in this release of CipherTrust Intelligent Remediation. Changing the PQS schema can corrupt data because GuardPoints do not migrate properly from the old schema to the new schema.

## Upgrade Considerations

- **Upgrade from 5.2.1.45 to 7.1.0.66**

  Upgrading from v5.x.x to 7.x.x is not supported. Only upgrading from 6.x.x to 7.x.x is supported due to new drivers added.

# Advisories

Veritas Cluster support will be dropped in CTE Agent v7.2.0.

# 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


Copyright © 2009-2021 Thales Group. All rights reserved.

# 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.**

Copyright © 2009-2021 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.


Copyright © 2009-2021 Thales Group. All rights reserved.