



# CipherTrust Transparent Encryption

## Patch Release Notes for Windows Agents

- **Release: 7.1.0.84**
- **Date: April 30, 2021**

## New Features and Enhancements

- Added support for Dell PowerMax storage for Efficient Storage GuardPoints.

## Resolved Issues

- **AGT-30022: After performing upgrades from 6.3.1.66 to 7.0.0.47, user could not enable the VERITAS cluster shared disk**  
After updating to the CTE build, the VERITAS cluster node could not be enabled due to a disk volume mounting issue. The issue is fixed in this agent build.
- **AGT-31439: Encrypted volumes with Efficient Storage, and greater than two terabytes in size, may not decrypt/data reduce correctly**  
Thales engineering has identified an issue in our AES XTS encryption algorithm when encrypted volumes are greater than two terabytes in size. Efficient storage customers will observe an impact to data reduction for disk LUNs with a size greater than 2TB. This issue is fixed in this release of CTE Agent.
- **AGT-31722 [CS1033618]: LDT rekey looping on DFSR cluster**  
The Live Data Transformation process excludes some system-specific files from the rekey process. On certain systems, deleted folders are called RECYCLER.BIN and on others they are called RECYCLER. The LDT process was trying to rekey the RECYCLER directory, where a system was preventing it from accessing or modifying its contents. The LDT process now excludes this system directory from the rekey process.
- **AGT-31806 [CS1038224]: CTE agent not validating the DSM or CM certificate**  
Fixed issue where Agent was not validating the server certificate from DSM or CipherTrust Manager.
- **AGT-31939 [CS1043167]: System crashing**  
Intermittently, CTE agent was not handling strings correctly that were non-NULL terminated. This gave CTE agent access to invalid memory.

- **AGT-32431 [CS1045438]: Windows BSOD when turning on debug log with high volume of transactions**

CTE agent was trying to access files before the Windows kernel had completely built those files. This caused an access violation due to invalid memory locations for those files.

- **AGT-32540 [CS1051095]: Received a 'digital signature signed drivers is required' message when installing v7.1.0.66 & v7.1.0.78**

The CTE agent's LFS driver was not attested correctly. This caused the Windows OS with secureboot enabled to throw the driver signing warning.

## Known Issues

- **AGT-32500: Registry values changed after MSI upgrade to 7.1**

**Workaround:** Add `IS_MINOR_UPGRADE=1` to the cmd line mentioned at step no 7:

```
msiexec.exe /i C:\msi_package\vee-fs-7.1.0-66-win64.msi /qn /norestart  
REINSTALLMODE=voums REINSTALL=ALL IS_MINOR_UPGRADE=1
```

## 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](mailto: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.**

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.