



CipherTrust Transparent Encryption for AIX

Release Notes

- **Release:** 7.2.0.56
- **Date:** February 04, 2022

New Features and Enhancements

Release 7.2.0.56 of CipherTrust Transparent Encryption (CTE) for AIX fixes known defects and addresses known vulnerabilities. For operating system and framework version support, see the [CTE Agent Compatibility Matrix](#).

Dynamic Host Setting

- The dynamic host setting now permits the modified host settings to take effect when the new entries are pushed from the DSM or CipherTrust Manager to the agent. Additionally, three new commands allow you to enable, disable and report the status of the dynamic host setting.

Encryption Key Protection

- Kernel Key Protection is now available for AIX. This allows CipherTrust Manager to encrypt keys that are cached in kernel memory. Previously, it was only available on Linux.

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-27295: Agent installer should not proceed with upgrade when it detects busy GuardPoints**

This has been fixed. The installer does not proceed when it detects a busy GuardPoint.

Note: This has not been fixed for raw devices.

- **AGT-31888 [CS1039694]: AIX 7.2 crashing when mounting NFS volume**

This has been fixed for directory and file system GuardPoints. A new function call was implemented to accommodate NFS volumes.

- **AGT-33343 [CS1049617]: Multiple dataforms ran against a single GuardPoint and caused corruption because of locking issues**

The dataform concurrent execution code was broken. This allowed multiple instances of dataform to run simultaneously on the GuardPoint. This has been fixed.

- **AGT-34908 [CS1073366]: An intercept code incorrectly truncated a value argument and caused the system call to fail**

The SecFS2 kernel module improperly called the `sigqueue()` AIX system call kernel interface. This truncated the system call argument which then sent an erroneous result to Java, which caused the WebSphere Application Server to fail. The type for the argument has been changed to fix this problem.

- **AGT-35418: Failed to bring up Oracle DB after doing data transformation from CS1 to CBC or CLEAR keys**

The relevant call was not setup to accommodate large files. This has been fixed.

- **AGT-36207 [CS1081031]: AIX Server Crash reported after CTE installation**

The agent was not using the latest kernel module loaded. This has been fixed.

- **AGT-37427 [CS1084169]: A compliance scan of port 7024 reported compliance issues with some TLS ciphers**

New, compliant TLS ciphers were added to the software and non-compliant TLS ciphers were removed.

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

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 © 2009-2022 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.