CipherTrust Transparent Encryption

Patch Release Notes for Linux Agents

- **Release: 7.0.0.88**
- **Date: January 15, 2021**

New Feature Support

The CTE Agent for Linux can now be installed on systems using UEFI Secure Boot. For details about using this feature, see "CTE Agent Installation with UEFI Secure Boot" on the next page. Documentation for this feature can also be found in versions 5 and higher of the 7.0.0 *CTE Agent for Linux Advanced Configuration and Integration Guide*, available at thalesdocs.com.

Resolved Issues

- **AGT-30885: Disable CTE-Efficient Storage feature during registration if XTS mode is not supported**

  Systems without AES XTS support should not allow the CTE-Efficient Storage feature to be installed because CTE-Efficient Storage requires XTS encryption keys.

  With this release of the CTE Agent, the DSM will disable the ES check box if the machine does not support XTS.

- **AGT29947 [CS1004144, CS1005946]: Need Secure Boot Support for CTE**

  Previous releases of the CTE Agent could not be installed on systems using UEFI Secure Boot because there was no matching public certificate that could be installed to certify the installation files.

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

CTE Agent Installation with UEFI Secure Boot

If you want to install the CTE Agent software on a Linux system that has UEFI Secure Boot enabled, you must first download the appropriate Thales public certificate and add that certificate to the MOK (Machine Owner Key) list on the host.

> **Note**
> The Thales public certificate is valid for three years from the date of issuance. Six months before the current public certificate is set to expire, Thales will release an advisory along with the new certificate that will become valid after the six month grace period expires. You can add the new certificate to the MOK list on all UEFI Secure Boot hosts any time before the old certificate expires and CTE will automatically start using the new certificate when the old certificate expires.

Public Certificate Naming Convention

The Thales public certificate name is `CTE_Secure_Boot_Cert_MM-DD-YYYY.der`. For example, `CTE_Secure_Boot_Cert_01-11-2021.der`.

Getting the Current Public Certificate

You can get the current public certificate in any of the following ways:

- From the CTE Agent installation file using the `-e` option. For example:

  ```
  # ./vee-fs-7.0.0-88-rh8-x86_64.bin -e
  Contents extracted.
  # ls | grep CTE_Secure_Boot_Cert
  CTE_Secure_Boot_Cert_01-11-2021.der
  ```

- From the Thales public directory https://packages.vormetric.com/pub/CTE_Secure_Boot/ or from the Thales Customer Support Portal (under KB0023449). The certificate on these sites is in PEM format, and must be converted to DER format before it can be added to the MOK list.

  For example, if the current certificate name is `CTE_Secure_Boot_Cert_01-11-2021.pem`, you could convert the certificate using the following command:

  ```
  # openssl x509 -inform PEM -outform DER -in CTE_Secure_Boot_Cert_01-11-2021.pem \
  -out CTE_Secure_Boot_Cert_01-11-2021.der
  ```

Adding the Certificate to the MOK List

> **Note**
> During this procedure, you will need to reboot the Linux host and then respond to a system prompt as soon as the host restarts. Make sure that all users accessing the host know that it will reboot and that you can respond to the system prompt as soon as the host restarts.

1. Log into the host as `root`.
2. Use the `mokutil --import <cert-name>` command to add the certificate to the MOK list. For example, if the certificate name is `CTE_Secure_Boot_Cert_01-11-2021.der`, you could enter:

   ```
   # mokutil --import CTE_Secure_Boot_Cert_01-11-2021.der
   ```

3. Enter and confirm a password for this request when prompted.

4. Reboot the host and follow the instructions on the console when the host comes back online. You will need to enter the password you created in the previous step.

   If you do not respond to the system prompt to update the MOK when the host restarts, the prompt will time out and you will need to run the `mokutil` command again.

5. When prompted, reboot the host again.

6. After the host has been rebooted the second time you can verify that the certificate has been properly added to the MOK list using the `mokutil --test-key` command. For example:

   ```
   # mokutil --test-key CTE_Secure_Boot_Cert_01-11-2021.der
   CTE_Secure_Boot_Cert_01-11-2021.der is already enrolled
   ```

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.