THALES

CipherTrust Transparent Encryption

Lifecycle & OS Support Guidelines

Release 7.2.0

Documentation Version 3

April 25, 2022

Lifecycle & OS Support Guidelines
7.2.0
April 25, 2022

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.

Overview

CipherTrust Transparent Encryption, formerly Vormetric Transparent Encryption, is an agent that runs in the kernel of an operating system. Due to the nature of the product, CipherTrust Transparent Encryption (CTE) has many updates per year. On average, there are approximately three feature releases per year. These releases contain major and/or minor new features or enhancements, support for new third-party databases or applications, and support for new major or minor versions of operating systems. During the rest of the year, Thales may release an update to CTE on an almost weekly basis in order to roll in new operating system kernel patch support and hot fixes. Following are the details of the CTE product lifecycle, as well as the CTE OS support guidelines.

CTE Release Types

The following table describes the CTE release types.

CTE Release	Major	Service Pack	Cumulative Patch	Hot Fix or New Kernel Support Build
Numbering	1.0.0	1.1.0	1.1.1	1.1.0.x
Cadence	3+ Years	6 Months	As needed	As needed
Contents	Major change in functionality	New features, fixes, major or minor OS support	New minor features, fixes, minor OS support	Hot fix or minor OS support, kernel updates if new CTE build is needed

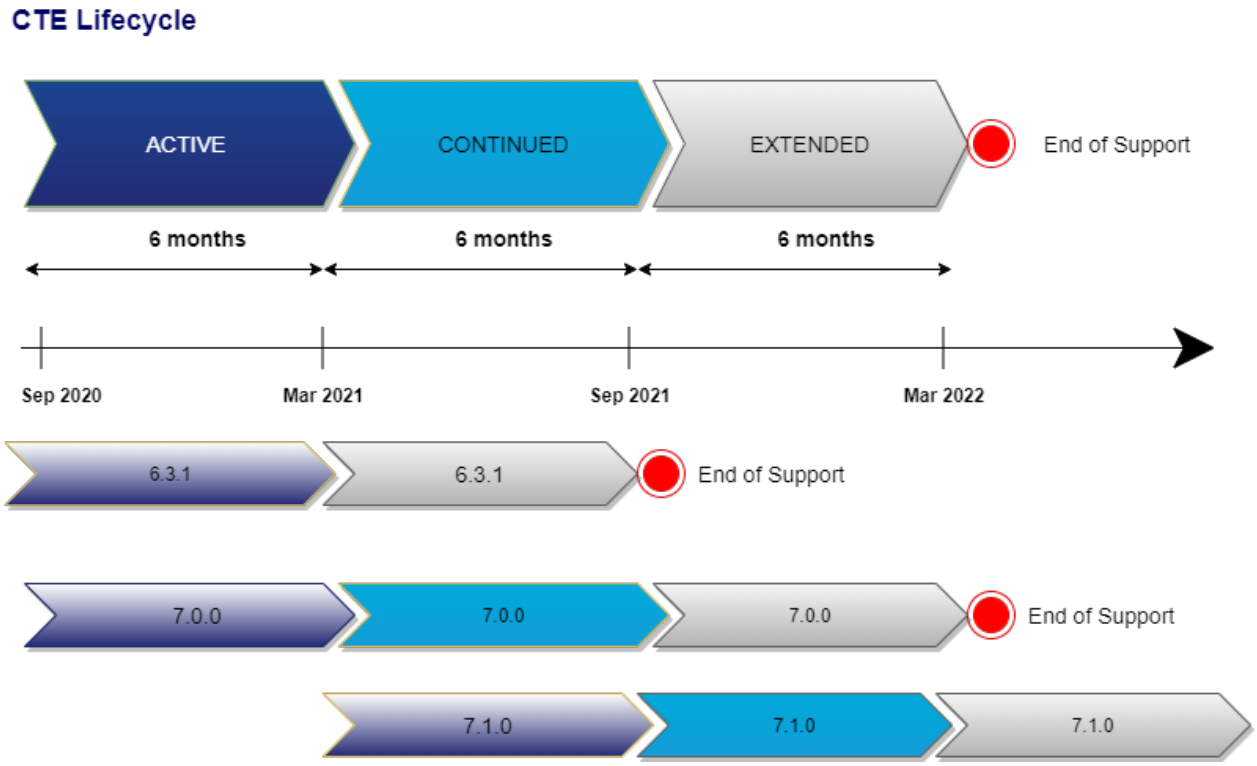
CTE Support Phase Definitions

The following table contains the CTE support phase definitions.

Support Phase	Definition	Timeframe
Active	Period during which Thales customer support assists customers with issues. A maintenance agreement makes the customer eligible for patches, and service packs.	From GA to the start of Continued Support
Continued Support	Customer support can be engaged mainly for troubleshooting and workarounds. Thales engineering will fix bugs and provide validation for new OS kernels and new minor OS releases on an as-need basis. However, no additional investment will be made by development and engineering departments.	Begins with the release of the next Service Pack; Ends after 6 months.
Extended Support	Support provided on an as-needed basis. An extended maintenance agreement must be in place. Thales will provide bug fixes only.	Only applies to the last Service pack before a Major release. Support time frame begins after Continued Support ends and lasts 6 months.

CTE Life Cycle

Following is a diagram of the CTE Life cycle. The version numbers are an example. They are not valid version numbers. The actual release time lines for these versions of CTE may be different. In general, there will be two “live” CTE versions at a time: one CTE version that is in active phase, and one that is in the Continued Support phase. In some cases, a third CTE version will also be in the extended support phase. This is to allow customers more time to move to the newer versions.



LTHF = Linux Taxonomy & Hot fix

Linux Taxonomy refers to the qualification of new Linux kernel releases with CTE.

When a cumulative patch is released for a CTE version that will be considered as the **active** CTE version, the current active service pack version and the previous service pack release continue to be supported for the continued support period. For instance, for the two active CTE versions 7.0.0 and 7.1.0, if a cumulative patch for 7.1.1 is released, CTE 7.1.1 and CTE 7.1.0 would be the supported versions for hot fixes.

CTE OS Support Guidelines

CTE supports the latest TWO major versions of an OS, for example RedHat Enterprise Linux 7 & 8, at any given time. CTE also supports the latest minor version (or Service Pack) of a major OS. Two examples are RedHat Enterprise Linux (RHEL) 7.9 and RHEL 8.4. Thales will qualify new kernel patches on the most recent minor or service pack version of an OS only. This mainly applies to Linux operating systems where kernel compatibility is critical. CTE is generally compatible with new kernel patches for any OS, but Linux creates patches more frequently and there is a higher probability for incompatibility. Refer to the CTE compatibility matrices for the complete list of supported operating systems.

CTE Compatibility Portal

The online compatibility portal lists all of the supported operating system kernels. Access it at the following link: https://thalesdocs.com/ctp/cte/cte-cm/index.html

In addition, go to https://packages.vormetric.com/pub/ to download a JSON file of all of the CTE supported kernels. Upload this file to your Key Manager,Vormetric Data Security Manager or the CipherTrust Manager, to monitor CTE agent compatibility. Request credentials to the packages repository from the Thales support team.

The CTE compatibility portal and matrix documents are updated with every CTE release & posted to the CTE documentation website: https://thalesdocs.com/ctp/cte/Books/Online-Files/index.html

OS Kernel Validation Process

Operating system vendors (especially Linux) release new kernel patches very frequently. Thales will automatically pick up these kernel patches, and test them with the latest version of CTE. In the majority of cases, CTE will not need an update to support a new kernel patch. Once validation is completed, Thales will announce kernel support with the current CTE version, or release a new build. Keep in mind that Thales will test kernel patches from the latest service pack (or minor version) of the two most recent major OS versions. The compatibility matrices will be updated (including the JSON file version) with the new kernel support, and if a new build is required, it will be posted for download from the Thales repositories.

Extended Update or Long-Term Support Kernels

Thales does not regularly validate kernel patches from OS versions that have entered extended update (EUS) or long-term support phases. This is in keeping with the policy of supporting the latest two major, and the latest minor version, of an OS. However, OS vendors are required to patch vulnerabilities in their software even if the OS has gone into an extended support or long-term support phase of the lifecycle. They are frequently releasing new kernel patches to their customers on these extended support branches. For this reason, Thales will validate EUS kernels for RHEL and LTSS kernels for SUSE, on a case-by-case basis using a “one-off” (or manual) validation process.

The following tables contain information on the validation processes for the OS distributions.

RedHat Enterprise Linux

The following table contains information on the Thales support for RHEL with CTE.

RH Linux Release	Thales Release	Timeframe for support (from the time of GA by vendor)	Example	Comment
Major	Next major or service pack CTE release	4 Business Days	RHEL 8	Major OS releases typically include significant kernel enhancements, new features and file systems.
Minor/Service Pack	Next major, service pack, or cumulative patch CTE release	4 Business Days	RHEL 8.4	OS Service pack or update releases do not include significant new features but on occasion break kernel binary compatibility.
Critical kernel security patch	Next CTE release, any type	4 Business Days		In exceptional cases, when more than 4 days are required, Thales will inform customers of the planned release date.
One-off EUS Kernel	Next CTE release, any type	30 Business Days		Must have Product Management approval; contact Thales support to request a one-off validation.

EUS: Extended Update Support

SUSE Linux Enterprise Server

The following table contains information on Thales support for SUSE Linux with CTE. Thales does not generally support long-term service pack support kernels (LTSS).

SUSE Linux Release	Thales Release	Timeframe for support (from the time of GA by vendor)	Example	Comment
Major	Next major or service pack CTE release	Up to 90 business days	SLES 15	Major OS releases typically include significant kernel enhancements, new features and file systems.
Minor/Service Pack	Next major, service pack, or cumulative patch CTE release	Up to 60 business days	SLES 15 SP1	OS Service pack or update releases do not include significant new features but on occasion break kernel binary compatibility.
Critical kernel security patch	Next CTE release, any type	Up to 20 business days		In exceptional cases, when more than 20 days are required, Thales will inform customers of the planned release date.
One-off LTSS kernel	Next CTE release, any type	Up to 30 business days		Must have Product Management approval; contact Thales support to request a one-off validation.

LTSS: Long-term Service Pack Support

Ubuntu Server Linux

LTS releases only

Thales Ubuntu support includes an exception. Thales will support **two** kernel series on the latest two major versions: e.g., the GA kernel and the HWE (hardware enablement) kernel series.

Ubuntu Linux security patches often break compatibility, and require a new build of CTE. Thales will release a new build according to the SLA noted below. The “one-off” kernel validation process does not apply to Ubuntu.

Ubuntu Linux Release	Thales Release	Timeframe for support (from the time of GA by vendor)	Example	Comment
Major	Next major or service pack CTE release	Up to 90 business days	Ubuntu 20.04	Major OS releases typically include significant kernel enhancements, new features and file systems.
Minor/Service Pack	Next major, service pack, or cumulative patch CTE release	Up to 60 business days	20.04.1	OS Service pack do not include significant new features but on occasion break kernel binary compatibility.
Critical kernel security patch	Next CTE release, any type	Up to 60 business days		In exceptional cases, when more than 30 days are required, Thales will inform customers of the planned release date.
New kernel series	Next major or service pack CTE release	Up to 60 business days		

Windows

The following table contains Thales support information for the Windows operating system with CTE. Thales supports both Windows Server and Windows Client versions. Check the Thales compatibility matrix for the list of supported operating systems.

Windows Release	Thales Release	Time frame for support (from the time of GA by vendor)	Example	Comment
Major/Long-term servicing channel	Next major or service pack CTE release	Up to 90 business days	Windows 2019	Windows long-term servicing channel releases typically include significant enhancements, new features and file systems.
Semi-annual channel releases	Next major, service pack, or cumulative patch CTE release	Up to 60 business days		Semi-annual channel releases do not include significant new features, but on occasion break kernel compatibility.
Security, Cumulative Patches	N/A	N/A		Windows patches rarely break compatibility. No CTE update required.

> **Note**
> CTE Windows will drop support for Operating systems when end of support is announced by Microsoft for an Operating system.

AIX

The table below contains Thales support information for the AIX operating system with CTE.

AIX Release	Thales Release	Timeframe for support (from the time of GA by vendor)	Example	Comment
Major	Next major or service pack CTE release	Up to 180 business days	AIX 8.1	Major releases typically include significant kernel enhancements, new features and file systems.
Technology Level	Next major, service pack, or cumulative patch CTE release	Up to 90 business days	AIX 7.2 TL1	Technology Level releases do not include significant new features but on occasion break kernel binary compatibility.
Kernel & Security patches or service pack for Technology Level	Next major, service pack, or cumulative patch CTE release	Up to 30 business days	AIX 7.2 TL1 SP5	Kernel patches or TL SP typically do not break compatibility. When they do, Thales will release a new CTE patch.

CipherTrust Transparent Encryption UserSpace

Overview

CTE UserSpace (formerly SafeNet ProtectFile FUSE) is a file-system level transparent encryption solution that leverages the cryptographic and key management features of the CipherTrust Manager platform to protect unstructured data. CTE UserSpace is based on Linux FUSE and hence, is not required to be updated when there is a Linux kernel update from the OS vendor. Following are the details of the CTE UserSpace product lifecycle.

CTE UserSpace Release Types

The following table describes the CTE UserSpace support phase definitions.

CTE Release	Major	Service Pack	Cumulative Patch
Numbering	1.0.0	1.1.0	1.1.1
Cadence	3+ Years	6 Months	As needed
Contents	Major change in functionality	New features, fixes, major or minor OS support	New minor features, fixes, minor OS support

CTE UserSpace Definitions

Support Phase	Definition	Timeframe
Active	Period during which Thales customer support will assist customers with issues. A maintenance agreement will make the customer eligible for patches, and service packs.	From GA to the start of Continued Support.
Continued Support	Customer support can be engaged mainly for troubleshooting and workarounds. Thales engineering will provide bugs and security fixes on an as-need basis. No additional investment will be made by development and engineering departments.	Begins with the release of the next Service Pack; Ends after 6 months.
Extended Support	Support provided on an as-needed basis. An extended maintenance agreement must be in place. Thales will provide bug fixes only.	Only applies to the last Service pack before a Major release. Support timeframe begins after Continued Support ends and lasts 6 months.

Appendix A: Extended support considerations

Support changes for Red Hat Enterprise Linux v7 with CipherTrust Transparent Encryption

In May, 2022, Red Hat plans to release a new major version of its Enterprise Linux operating system: v9. Thales was able to begin supporting Red Hat Enterprise Linux (RHEL) 9 immediately with CTE version 7.2.0 as a participant in the Early Adopter Program (EAP). It is now time to prepare for the removal of support for RHEL v7. Thales tries to maintain the operating system support policy of providing support with CTE of the two latest major versions of an operating system as outlined in this guide. Accordingly, Thales will shift to a One-Off manual qualification process on a need basis only for RHEL 7.9 kernels once RHEL 9 is GA. Thales understand that this is a highly adopted and widely used operating system, so Thales is willing to extend CTE support for a grace period to allow customers to move their RHEL 7 systems to a newer version before removing support.

According to Red Hat support portal, End of “Maintenance Support 2 (Product Retirement)” from Red Hat for RHEL 7 will be June 30, 2024. Thales would like to align, as best as possible, to this date.

Thales will review the need for supporting RHEL 7 during the Extended Lifecycle Support (ELS) which ends, June 30, 2026, and it will only be available to customers with additional extended support contracts for CTE agents.

Thales will provide priority bug fixes on an as-needed basis and technical support for customers with paid support contracts. Thales will not add any new features, enhancements, performance improvements, update third party databases or provide application interoperability support on the CTE agents for RHEL 7.