



Sentinel LDK 10.2 with Sentinel LDK- EMS

RELEASE NOTES



Revision History

Part number 007-002029-001, Revision C, 2511-1

Disclaimer and Copyrights

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries and 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 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 publicly accessible 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 © 2025 THALES. All rights reserved. Thales, the Thales logo and Sentinel 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.

CONTENTS

Sentinel LDK 10.2 with Sentinel LDK-EMS Release Notes	5
Release: 10.2 November 2025	5
Product Overview	6
Sentinel Vendor Keys	6
New Features, Enhancements, and Changes	7
Release: 10.2	7
Fingerprint Generation API for Windows and Linux	7
Support for Remote Developer Key with Envelope	8
Enhanced Envelope Support for .NET Core Application Assemblies	9
Sentinel LDK Data File Protection Write Support for Linux	9
Enhanced Sentinel LDK Envelope Protection for Python Applications Under Linux and Windows	9
Vendor Code Can Be Excluded From Sentinel LDK Envelope Project File	9
Enhanced Control for Disabling Secure Storage ID Check	10
Installation and Upgrades	11
Installing Windows, Linux, and macOS Packages	11
Upgrading an Earlier Version of Sentinel LDK	11
Security Updates	12
Reporting a Security Vulnerability	12
Supported Platforms	13
Sentinel LDK Run-time Environment (RTE) – Supported Versions	13
RTE and the Version Enforcement Option	14
Sentinel LDK Run-time Environment (RTE) and Protected Applications – Supported Platforms for End Users	15
Support for Creating Detached SL UserMode Licenses	18
Web Servers for Java Applications with Method-Level Protection	19
Web Browsers for Sentinel Admin Control Center	19
Sentinel LDK-EMS Service	20
Sentinel LDK Vendor Tools	21
Vendor Library Version Dependency	23
Supported Platforms for Code Samples	26
Tested Compilers for Code Samples	26
Current Firmware Version	30
Documentation	31
Online Documentation	31

Locally Installed Documentation	31
Software Protection and Licensing	31
Tutorials and Quick Start Guides	32
Migration Guides	32
Sentinel LDK-EMS	33
Getting Started Guides for Non-Windows Platforms	33
Sentinel LDK and Sentinel LDK-EMS User Interfaces	34
Sentinel LDK APIs	35
Resolved Issues	36
Release: 10.2	36
Known Issues and Workarounds	37
Sentinel LDK Installation and Software Manager	37
Sentinel LDK-EMS	38
End Users, Sentinel LDK Run-time Environment, License Manager, and Customer Tools	39
Sentinel LDK Envelope and Data Encryption for Windows Platforms	41
Sentinel LDK Envelope and Data Encryption for Linux	45
Sentinel LDK Envelope, Data Encryption, and Licensing API for macOS	46

Sentinel LDK 10.2 with Sentinel LDK-EMS Release Notes

These release notes are subject to change. If you are reading the release notes that were installed with the product, Thales recommends that you check the release notes available online to see if any information was added or changed. You can access the latest release notes from: [Sentinel LDK Release Notes](#)

Translations coming soon!

[View the previous version](#) in English of the release notes.

[Download a ZIP file](#) in English with all Sentinel LDK release notes.

Release: **10.2** | November 2025

- > ["New Features, Enhancements, and Changes" on page 7](#)
- > ["Installation and Upgrades" on page 11](#)
- > ["Security Updates" on page 12](#)
- > ["Supported Platforms" on page 13](#)
- > ["Documentation" on page 31](#)
- > ["Resolved Issues" on page 36](#)
- > ["Known Issues and Workarounds" on page 37](#)

Product Overview

Sentinel LDK is Thales' industry-leading software protection and licensing solution. It provides cutting edge security technologies for the utmost in copy protection, a range of license models and entitlement fulfillment options, and out-of-the-box tools which facilitate quick integration and deployment. Sentinel LDK supports hardware-based, software-based and cloud-based licensing and includes a range of APIs to allow software vendors to automate and tailor the implementation to their unique business requirements.

The strength, uniqueness, and flexibility of Sentinel LDK are based on two primary principles:

- > *Protect Once—Deliver Many—Evolve Often™* — this unique design philosophy enables you to fully separate your business and protection (engineering) processes in order to maximize business agility while ensuring optimum use of your employee time and core competencies, resulting in faster time to market.
- > *Cross-Locking™* — the technology that supports the *Protect Once—Deliver Many—Evolve Often* concept, enabling a protected application to work with a Sentinel hardware key or a Sentinel License Certificate (software key).

All commercial decisions, package creation and license definitions are executed by product or marketing managers after the protection has been implemented.

This workflow model provides you with greater flexibility and freedom when defining new sales and licensing models, including feature-based and component licensing, evaluation, rental, floating, subscription, trialware, pay-per-use, and more, enabling you to focus on revenue growth.

Sentinel Vendor Keys

When you purchase Sentinel LDK, you are provided with two Sentinel Vendor keys—the Sentinel Developer key and the Sentinel Master key.

The Sentinel Developer key is used by your software engineers in conjunction with the Sentinel LDK protection tools to protect your software and data files.

The Sentinel Master key is only required if you install Sentinel LDK-EMS on premises. It is used in conjunction with Sentinel LDK and is attached to the Sentinel LDK-EMS Server. This key is used by your production staff to create licenses and lock them to Sentinel protection keys, to write specific data to the memory of a Sentinel protection key, and to update licenses already deployed in the field.

Important: The Master key is especially valuable because it is used to generate licenses. Both Vendor keys contain secrets and enable the use of tools and API libraries which can access the memory of user keys and use of the cryptographic functionalities.

New Features, Enhancements, and Changes

> ["Release: 10.2 " below](#)

NOTE If you are upgrading from a version of Sentinel LDK that is earlier than 10.0, be sure to review the release notes for all intervening versions. Significant enhancements and changes are introduced in each version of Sentinel LDK. [Download a ZIP file](#) that contains all Sentinel LDK release notes to see the changes.

Release: 10.2

In this section:

- > ["Fingerprint Generation API for Windows and Linux" below](#)
- > ["Support for Remote Developer Key with Envelope" on the next page](#)
- > ["Enhanced Envelope Support for .NET Core Application Assemblies" on page 9](#)
- > ["Sentinel LDK Data File Protection Write Support for Linux" on page 9](#)
- > ["Enhanced Sentinel LDK Envelope Protection for Python Applications Under Linux and Windows" on page 9](#)
- > ["Vendor Code Can Be Excluded From Sentinel LDK Envelope Project File" on page 9](#)
- > ["Enhanced Control for Disabling Secure Storage ID Check" on page 10](#)

Fingerprint Generation API for Windows and Linux

Sentinel LDK now supports the generation of a machine fingerprint for machines in situations where outgoing file transmission is restricted (for example, for air-gapped machines).

A user can determine the required hardware identifiers data for generating a license on the target machine and share the data with you by telephone or email. You enter the provided data in to the Fingerprint Generator API (on a Windows and Linux ARM machines) to generate a C2V file. The C2V file can then be passed to Sentinel LDK-EMS, which will use the C2V to generate a V2C or V2CP file to install an SL AdminMode or SL UserMode license on the target machine.

The user can provide one or more of the following hardware identifiers for generating the license:

- > MAC address
- > FQDN (Fully Qualified Domain Name)

- > IP address
- > SID (Security Identifier on Windows or System ID on Linux)

The Fingerprint Generator API enables you to:

- > Support environments where C2V files cannot be shared due to security restrictions.
- > Generate fingerprints that are compatible with both Windows and Linux platforms.
- > Generate fingerprints for both physical machines and virtual machines.
- > Validate the accuracy of manually provided entered hardware identifier using checksum characters. The checksum is optional. If omitted, the API accepts the identifier as is and skips checksum validation.

When generating a fingerprint file, consider the following:

- > Security decreases when using fewer components (for example, using only MAC address or only FQDN).
- > If the SSID (Secure Storage Identifier) is not provided, Thales recommends that you use **Perpetual** or **Expiration Date** licenses for enhanced security to avoid possible license abuse.
- > When generating a license using the fingerprint generated by the API, you **must use the custom clone protection scheme**. This ensures compatibility with the fingerprint data and prevents license misuse or cloning.

For more information, see [Sentinel LDK Software Protection and Licensing Guide](#).

Support for Remote Developer Key with Envelope

The Sentinel LDK License Manager now supports the use of a remote Developer key with Envelope.

Envelope (V3, .NET, Java, and Linux) and Data File Protection tools (dfcrypt and Data Protection utility) now support using a Developer key connected to a remote machine within the same network.

This enhancement enables multiple engineers to share a single physical Developer key without requiring individual keys. It simplifies collaborative development and build automation, and allows you to integrate Envelope protection into build environments that do not have USB connectivity.

Only Developer keys support remote access. Master keys support only local use.

NOTE

- > In an environment where developers or build servers are using remote Developer keys: You must implement a process to ensure that the relevant development machines or build servers always have the most recent downloaded API libraries.
- > The Master Wizard does not support using a remote Developer key. A local Developer key or Master key must be connected during the Master Wizard introduction process.

To enable remote access for a Developer key, contact your Thales representative.

Enhanced Envelope Support for .NET Core Application Assemblies

Sentinel LDK Envelope has been enhanced to support the Windows shell protection feature for .NET Core Main assemblies.

For these assemblies, Linux is now also supported for Linux Intel (x86_64), Linux ARMHF, and Linux ARM64.

Sentinel LDK Data File Protection Write Support for Linux

Sentinel LDK Data File Protection (DFP) for Linux now includes full read and write support. This enhancement adds mmap-based file access and allows combining mmap with standard file I/O.

As a vendor developing a Linux application that uses DFP to encrypt data files, you can now create new encrypted files, specify file name patterns for encryption, and assign a feature ID for each file. If no feature ID is specified, the default value of 0 is used.

The `input_glob` and `ignore_glob` parameters use the same pattern syntax as the JSON configuration file in Script Envelope.

This enhancement enables you to protect and modify data files on Linux Intel and ARM platforms (32-bit and 64-bit), improving workflow efficiency and flexibility.

Enhanced Sentinel LDK Envelope Protection for Python Applications Under Linux and Windows

Script Envelope for Python applications (under Windows or Linux) now supports the optional **`entry_scripts_glob`** parameter in the project file.

You can use this parameter in your Script Envelope project file to specify one or more entry scripts for your Python project.

Script Envelope generates stub code to ensure that the runtime libraries load correctly. The behavior of stub generation depends on whether you specify the **`entry_scripts_glob`** parameter.

This enhancement reduces unnecessary stub files, enforces valid entry scripts, and helps vendors ensure that the runtime loads correctly for the intended entry scripts only.

For more details, see [Sentinel LDK Envelope for Linux](#) or [Sentinel LDK Envelope for Windows](#).

Vendor Code Can Be Excluded From Sentinel LDK Envelope Project File

You can now prevent Sentinel LDK Envelope from caching the Vendor Code in the Sentinel LDK Envelope project file.

The Vendor Code is used by Envelope to protect applications and by the Data Protection utility to protect data files. Envelope retrieves the Vendor Code either from a location on the file system or from the Sentinel LDK-EMS database, depending on the option that you select in the he Sentinel Vendor Code screen. Until now, Envelope

would always cache the retrieved Vendor Code in the project file for subsequent sessions regardless of how the Vendor Code was obtained. The cached Vendor Code was then used by Envelope GUI, by the Envelope command-line version, and by the Data File Protection utility.

Effective with the release of Sentinel LDK Envelope 10.2, when you select the option to retrieve the Vendor Code from the Sentinel LDK-EMS database:

- > To work with Envelope, you are required to provide login credentials to access Sentinel LDK-EMS. When the Vendor Code is required, Envelope will retrieve the Vendor Code from Sentinel LDK-EMS. The Vendor Code is not be cached in the Envelope project file. For details, see [Sentinel LDK Envelope for Windows](#).
- > The Data File Protection utility obtains the Vendor Code from Envelope if an active session of Envelope exists. If an active session of Envelope does not exist, the Data File Encryption Utility requires you to provide login credentials to access Sentinel LDK-EMS.
- > When working with the Envelope command-line version, you must provide login credentials to access Sentinel LDK-EMS. For details, see [Sentinel LDK Envelope for Windows](#).
- > When working with an Envelope project file created by an earlier version of Sentinel LDK Envelope, the cached Vendor Code is removed from the project file.

When you select the option to retrieve the Vendor Code from a location on the file system, Envelope continues to cache the Vendor Code in the project file.

Enhanced Control for Disabling Secure Storage ID Check

You can disable the Secure Storage ID (SSID) check by adding the `<ignore_secure_storage_id_check>` tag in the license while license generation.

This tag applies only to Features that use the license models you specify. This tag behaves as follows:

- > Perpetual Features remain enabled regardless of this tag.
- > The SSID check is disabled for the Default Feature (FID 0) if you include the global option under `<license_properties>`.

For details, see the topic "How to disable Secure Storage ID Check" in the [Sentinel License Generation API Reference](#).

Installation and Upgrades

Visit the [Thales Customer Support Portal for Sentinel LDK](#) for the most recent versions of Sentinel LDK software and included documentation.

In this section:

Installing Windows, Linux, and macOS Packages

The Sentinel LDK installation includes the files required for Windows, Linux, and Mac platforms.

For Linux and macOS, the required files are available on the machine where Sentinel LDK for Windows is installed, under the following path:

`%ProgramFiles(x86)%\Thales\Sentinel LDK\Additional Platforms\`

Alternatively, you can download all Sentinel LDK installation packages, including separate ones for Windows, Linux, and Mac platforms from the Thales Support Portal at the following location:

> https://supportportal.thalesgroup.com/csm?id=kb_article_view&sys_kb_id=c2241c1d1bb41890f12064606e4bcb3e&sysparm_article=KB0021845

Upgrading an Earlier Version of Sentinel LDK

Instructions for upgrading from earlier versions of Sentinel LDK can be found in the [Sentinel LDK Installation Guide](#).

Considerations when upgrading Sentinel LDK:

- > When upgrading to Sentinel LDK 10.2 from Sentinel LDK v.7.3 through v.7.8, all non-English locales of Customer contacts and Channel Partner contacts in Sentinel LDK-EMS are converted to the English locale. If this issue is applicable to your installation of Sentinel LDK-EMS, make sure to read [this technical note](#) before upgrading to Sentinel LDK 10.2.

NOTE You can ignore this issue if all of your Customer contacts and Channel Partner Contacts are set up to use the English locale or if you are not upgrading Sentinel LDK-EMS.

- > The procedure for upgrading to Sentinel LDK 10.2 has been tested only for Sentinel LDK v.8.5 and later.

If you plan to upgrade from an earlier version of Sentinel LDK, contact Technical Support to validate the upgrade scenario. (This applies whether you are upgrading Sentinel LDK Vendor Tools, Sentinel LDK-EMS, or both.)

Security Updates

For the latest information regarding any older or newly-discovered issues, see:

<https://cpl.thalesgroup.com/software-monetization/security-updates>

Reporting a Security Vulnerability

If you think you have found a security vulnerability, please report it to Thales using the links in:

<https://cpl.thalesgroup.com/software-monetization/security-updates>

There are no known security issues at the time of this release, and this release does not resolve any known security issues relating to Sentinel products.

Supported Platforms

The operating system versions listed in this section were tested by Thales and verified to be fully compatible with Sentinel LDK. Older operating system versions are likely to be compatible as well, but are not guaranteed. For reasons of compatibility and security, Thales recommends that you always keep your operating system up to date with the latest fixes and service packs.

In this section:

- > ["Sentinel LDK Run-time Environment \(RTE\) – Supported Versions" below](#)
- > ["Sentinel LDK Run-time Environment \(RTE\) and Protected Applications – Supported Platforms for End Users" on page 15](#)
- > ["Support for Creating Detached SL UserMode Licenses" on page 18](#)
- > ["Web Servers for Java Applications with Method-Level Protection" on page 19](#)
- > ["Web Browsers for Sentinel Admin Control Center" on page 19](#)
- > ["Sentinel LDK-EMS Service" on page 20](#)
- > ["Web Browsers for Sentinel LDK-EMS" on page 21](#)
- > ["Sentinel LDK Vendor Tools " on page 21](#)
- > ["Vendor Library Version Dependency" on page 23](#)
- > ["Supported Platforms for Code Samples" on page 26](#)
- > ["Tested Compilers for Code Samples" on page 26](#)
- > ["Current Firmware Version" on page 30](#)

Sentinel LDK Run-time Environment (RTE) – Supported Versions

To support all of the latest enhancements in Sentinel LDK, and to provide the best security and reliability, Thales recommends that you provide end users with the latest RTE wherever the RTE is required.

Sentinel LDK Run-Time Environment version 10.21 is provided for Windows, Mac, and Linux (Intel and ARM) systems.

NOTE

- > **Cloud licensing.** Thales highly recommends that you always install the latest version of the RTE on the license server machine. (This is applicable for both vendors and customers who are hosting cloud licenses on their license server machine.)

If you downgrade the Run-time Environment after implementing cloud licensing, client identities or licenses may become unavailable. To resolve such issues, upgrade to the previously-installed RTE version or later.

- > **Upgrading.** Upgrading Sentinel LDK RTE to version 8.21 or later migrates existing SL AdminMode licenses to a new secure storage. Once this occurs, you cannot downgrade the RTE to an earlier version. Downgrading the RTE will make existing SL AdminMode licenses invalid.

RTE and the Version Enforcement Option

For all functionality existing in Sentinel LDK prior to the latest version, earlier versions of the RTE are supported as follows when using your customized vendor API libraries 10.21:

Version enforcement option	RTE requirements for end users
Version-restricted	Whenever the RTE is required, RTE 8.15 or later must be provided.
Version-unrestricted	The protected application does not check the version number of the RTE. Whenever the RTE is required, the RTE must be from a version of Sentinel LDK that supports the features that you are using to protect and license your applications.

For details, see "Required Version of the Run-time Environment" in the [Sentinel LDK Software Protection and Licensing Guide](#).

Sentinel LDK Run-time Environment (RTE) and Protected Applications – Supported Platforms for End Users

The RTE, and protected applications (with or without the RTE), can be installed under the following platforms or frameworks on end users' machines:

Platform or Framework	Supported Versions
.NET	<p>Sentinel LDK provides support for the following target frameworks:</p> <ul style="list-style-type: none">> .NET Framework: v4.0 - v4.8> .NET Standard: v2.1> .NET 6, 8, 9 <p>Protected applications that use the supported .NET frameworks are supported on the following platforms:</p> <ul style="list-style-type: none">> Windows (Win32 and x64)> Linux Intel (x86_64)> Linux ARMHF> Linux ARM64> Mac (only protected with Licensing API) <div>NOTE When protected with Envelope: .NET applications with platform-specific functionality such as Windows Forms and Windows Presentation Foundation (WPF) work only on Windows platforms.</div>

Platform or Framework	Supported Versions
Windows	<p>x86 and x64 versions of the following:</p> <ul style="list-style-type: none"> > Windows Server IoT 2019 > Windows Server 2022 > Windows Server IoT 2022 > Windows Server 2025 > Windows Server IoT 2025 > Windows 10 IoT Enterprise 2021 LTSC > Windows 11 IoT Enterprise 2024 LTSC > Windows 11 23H2 > Windows 11 24H2 (requires RTE 10.13) > Windows 11 ARM 24H2 (only protected with Licensing API) requires RTE 10.13 > Windows 11 ARM 25H2 <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>NOTE Support on Windows ARM machines with the ARM64-based processor:</p> <ul style="list-style-type: none"> > Sentinel LDK is supported via emulation. > Sentinel HASP keys and Sentinel HL (HASP configuration) keys are not supported. > Applications that are licensed with HASP4 or Hardlock keys are not expected to work. </div> <p>Note: Windows Insider Preview builds are not supported. The latest service packs and security updates must be installed.</p>
Mac	<ul style="list-style-type: none"> > macOS 13.6 Ventura > macOS 14.3 Sonoma > macOS 15 Sequoia <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Support on Mac machines with the ARM64-based processor:</p> <ul style="list-style-type: none"> > Sentinel LDK is supported via Rosetta 2. > Sentinel Licensing API version 8.41 and later is supported natively. </div> <p>Note: The Sentinel Remote Update System (RUS utility) is not supported for Mac systems. To obtain a fingerprint, use Sentinel Admin Control Center.</p>

Platform or Framework	Supported Versions	
Linux	Linux Intel (x86-64)	<ul style="list-style-type: none"> > OpenSUSE Leap 15.6 (requires RTE 10.13) > Red Hat EL 10 > Ubuntu Server 22.04, 24.04 > Ubuntu Desktop 22.04, 24.04 > Debian 13 > CentOS Stream 10 <p>The latest service packs and security updates must be installed.</p>
	Linux ARM 32-bit (armel and armhf)	<p>The following hardware/boards have been validated:</p> <ul style="list-style-type: none"> > BeagleBone Black > Raspberry Pi-4 > NI cRIO-9068
	Linux ARM 64-bit (arm64)	<p>The following hardware/board has been validated:</p> <ul style="list-style-type: none"> > Qualcomm DragonBoard 410c
	Wine	Sentinel LDK RTE was tested on Linux platforms with Wine 10.0
Android	Android ARM (64-bit)	Android 14.x, 15.x, 16.x
	Android Architecture	<p>The following architecture is supported:</p> <ul style="list-style-type: none"> > arm64
	Android ABI	<p>Sentinel LDK supports Android applications designed for the following Android application binary interface:</p> <ul style="list-style-type: none"> > arm64-v8a

Platform or Framework	Supported Versions
Virtual Machines	<p>The VM detection and VM fingerprinting capabilities provided by Sentinel LDK have been validated on the following technologies:</p> <ul style="list-style-type: none"> > Parallels Desktop 19 for Mac > VMware Workstation 17 > VMware ESXi 7.0, 8.0 > Hyper-V Server 2019 (SL only) > Xen Project 4.18 > KVM (RHEL 9.3, Ubuntu 24.04 server, Debian 12.5) > Microsoft Azure > VirtualBox 7.0 > Docker containers: <ul style="list-style-type: none"> • Fully supported for Linux, including under Kubernetes and with licenses installed inside the container. Limitation: The client side and license server cannot use the same IP address if licenses are installed outside the container. • Support for Windows is limited to consumption of licenses that contain multiple seats and that are installed outside the container. > LXC containers > Amazon EC2 > GCP Compute Engine > Alibaba Cloud Elastic Compute Service

Support for Creating Detached SL UserMode Licenses

You can use the Sentinel Licensing API (except for the REST API) to detach a license from an SL AdminMode key or CL key to an SL UserMode key.

Requirement Type	Prerequisites
Supported Host Platforms	<ul style="list-style-type: none"> > Windows > Linux > Linux Docker
Supported Target Platforms	<ul style="list-style-type: none"> > Windows > Android

Requirement Type	Prerequisites
Sentinel LDK Run-time Environment	Not required on the target device
Supported Detach Modes	<ul style="list-style-type: none"> > Auto-detach > On-demand detach
Protecting Applications	<ul style="list-style-type: none"> > Protect applications using a vendor-specific API (version 10.13 or later). > To support auto-detach for applications protected with Sentinel LDK Envelope: Set the LOCKING_TYPE parameter in Envelope to HL or SL (AdminMode or UserMode). (The default setting is HL or SL-AdminMode.)

Web Servers for Java Applications with Method-Level Protection

The following web servers are supported for Java applications that are protected with Sentinel LDK Envelope using method-level protection:

- > Tomcat 9.* and earlier
- > WildFly 26.* and earlier
- > Glassfish 5.1 and earlier
- > JBoss 7.4 and earlier

No limitations exist on web servers for Java applications with only class-level protection.

Web Browsers for Sentinel Admin Control Center

The latest versions of the following Web browsers are supported:

- > Microsoft Edge
- > Mozilla Firefox
- > Google Chrome
- > Safari

Sentinel LDK-EMS Service

This section describes requirements for Sentinel LDK.

Operating Systems

When installed on premises, Sentinel LDK-EMS Service is supported under the following operating systems:

System	Supported Versions
Windows	<p>x64 versions of the following:</p> <ul style="list-style-type: none">> Windows Server 2019> Windows Server 2022> Windows Server 2025> Windows 10 22H2> Windows 11 24H2 <p>Note: Windows Insider Preview builds are not supported.</p> <p>The latest service packs and security updates must be installed.</p>

Sentinel LDK-EMS Database

When installed on premises, the Sentinel LDK-EMS database is supported as follows:

System	Supported Database Server Software
Windows	<ul style="list-style-type: none">> Microsoft SQL Server 2017 Express> Microsoft SQL Server 2019 Express> Microsoft SQL Server 2022 Express <p>Note: Microsoft SQL Server 2019 Express Edition can be installed automatically by the Sentinel LDK-EMS Installation wizard. The installer for this version of Microsoft SQL Server is also available on the Sentinel LDK installation drive.</p> <p>Limitations: The Express editions of Microsoft SQL Server provide a maximum relational database size of only 10 GB. For details, see https://learn.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2016?view=sql-server-ver16#deciding-among-components.</p> <p>Check the LDK-EMS database size regularly so that you can take measures when database size is closer to 10 GB.</p> <p>If your database is approaching the 10 GB limitation, consider one of the following options:</p> <ul style="list-style-type: none">> Upgrade to SQL Server (paid version)> Migrate to Thales-hosted Sentinel EMS

Sentinel LDK-EMS Hardware Requirements

See [Sentinel LDK Installation Guide](#)

Web Browsers for Sentinel LDK-EMS

The latest versions of the following web browsers are supported with both HTTPS and HTTP:

- > Microsoft Edge
- > Mozilla Firefox
- > Google Chrome

NOTE The Mac Safari Web browser is *not* supported for Sentinel LDK-EMS (both Vendor Portal and Customer Portal).

Tomcat and JRE for Sentinel LDK-EMS

When installed on-premises, Sentinel LDK-EMS is compatible with the following:

- > **Tomcat:** 9.0.110 or later
- > **JRE:** OpenJDK 8.402

Sentinel LDK Vendor Tools

Important! You must always install the latest version of the Sentinel RTE on the machines that you use to work with Sentinel LDK Vendor Tools and Sentinel LDK-EMS. (Under Windows, the RTE is installed automatically as part of the Sentinel LDK installation procedure.)

System	Supported Versions
Windows	<p>x64 versions of the following:</p> <ul style="list-style-type: none">> Windows Server 2019> Windows Server 2022> Windows Server 2025> Windows 11 24H2 <p>Note: Windows Insider Preview builds are not supported.</p> <p>The latest service packs and security updates must be installed.</p> <p>Display: Requires a minimum screen resolution of 1280 by 1024 pixels with 24-bit color quality.</p> <p>Note for Sentinel LDK Envelope: To protect and execute the provided .NET sample application under Windows 8.1 or Windows Server 2012 R2, you must install Microsoft .NET Framework 3.5.</p>

System	Supported Versions
Mac	<ul style="list-style-type: none"> > macOS 14.3 Sonoma > macOS 15.x Sequoia <div> <p>For Mac machines with the ARM64-based processor: Vendor Tools (Envelope, Data Protection utility) are supported using the Rosetta 2 emulator. For more information on support for Envelope, see Sentinel LDK Envelope for Mac.</p> </div> <p>Applications built on the Cocoa framework are supported.</p> <p>Web Browsers for Sentinel Vendor Tools Help Systems:</p> <ul style="list-style-type: none"> > Mozilla Firefox > Mac Safari with configuration option Cross-Origin Restriction disabled. (This option can be accessed from the Developer menu.)
Linux Intel	<p>Sentinel LDK Envelope for Linux and Master Wizard for Linux are supported on the x86-64 version of the following distributions of Linux:</p> <ul style="list-style-type: none"> > OpenSUSE Leap 15.6 > Red Hat EL 10 > Ubuntu Server 22.04, 24.04 > Ubuntu Desktop 22.04, 24.04 > Debian 13 > CentOS Stream 10 <p>The latest service packs and security updates must be installed.</p>
Linux ARM	<ul style="list-style-type: none"> > ARM 32-bit > ARM 64-bit <p>Sentinel LDK Envelope for Linux (on a Linux Intel platform) can protect applications that will run on ARM 32-bit and ARM 64-bit platforms.</p>
Android	Android ARM platforms
Java	Java 8

Vendor Library Version Dependency

Your customized Vendor libraries (**haspplib_<vendorID>.***) are downloaded each time that you introduce one of your vendor keys to Sentinel LDK. You should re-introduce one of your vendor keys each time that you upgrade to a new version of Sentinel LDK.

This section describes dependencies for each version of the vendor libraries.

- > **When using the Admin License Manager:** The version of the RTE should normally be equal to or later than the version of the customized Vendor library unless specified otherwise (see rows below with multiple Vendor Library versions). For example:

Vendor Library Version	Required Run-time Environment Version
Older than 7.100	The vendor library is no longer supported. Upgrade to a supported version.
7.100	7.80 or later
8.11	8.11 or later
8.13	8.13 or later
8.15	8.15 or later
8.21	8.21 or later
8.23	8.23 or later
8.31, 8.32, 8.34	8.31 or later
8.41	8.41 or later
8.51	8.51 or later
9.12, 9.13, 9.15	9.12 or later
10.11	10.11 or later
10.12	10.12 or later
10.13	10.13 or later
10.14	10.14 or later
10.21	10.21 or later

NOTE A given version of the Vendor library is compatible with newer versions of the RTE. However, to support the enhancements in a given version of the RTE, the equivalent version of the Vendor library may be required.

- > **When using the External License Manager (hasp_rt.exe):** The following table indicates the version dependency of the customized Vendor library:

Vendor Library Version	Required External License Manager Version
7.100	23.0
8.11	24.0
8.13	24.2
8.15	24.4
8.21	25.0
8.23	25.2
8.31, 8.32, 8.34	26.0
8.41	27.0
8.51	28.0
9.12, 9.13, 9.15	29.1 or later
10.11	30.0 or later
10.12	30.1 or later
10.13	30.2 or later
10.14	30.3 or later
10.21	31.0 or later

NOTE Make sure that the Vendor library and External License Manager versions are synchronized according to the table.

You can download the latest External License Manager from the **Sentinel LDK Runtime & Drivers** link at: <https://cpl.thalesgroup.com/software-monetization/sentinel-drivers>

- > **When using the Integrated License Manager:** Your customized Vendor library is not required, so there is no version dependency.
- > **When using high-availability for cloud licensing:** The Vendor library version must be in sync with the LMS version. Older Vendor libraries are not supported.

The following table lists the supported versions of the Vendor libraries and the matching LMS (Run-time Environment) version:

Vendor Library Version	Matching LMS (Run-time Environment) Version
8.31, 8.32, or 8.34	8.31
8.41	8.41
8.43	8.43
8.51	8.51, 8.52, 8.53, 8.54
9.12, 9.13, 9.15	9.12 or later
10.11	10.11
10.12	10.12
10.13	10.13
10.14	10.14
10.21	10.21

Supported Platforms for Code Samples

The code samples are supported on the same platforms as listed for ["Sentinel LDK Vendor Tools " on page 21](#).

NOTE The **hasp_net_windows.dll** provided in the Licensing API vb.net and C# samples for Windows has been compiled with .NET Framework 4.5.

To work with this DLL, .NET Framework 4.5 or later must be installed on your machine.

Prior to Sentinel LDK v.7.4, this DLL was compiled with .NET Framework 2.0, which is now known to contain security vulnerabilities. Because of these vulnerabilities, Thales highly recommends that you upgrade to .NET Framework 4.5 or later.

If you do not want to upgrade your old .NET Framework, you can obtain and use the **hasp_net_windows.dll** for Windows from a Sentinel LDK release earlier than v.7.4. To obtain an earlier version of Sentinel LDK, contact Technical Support.

Tested Compilers for Code Samples

API	Programming Language	Tested Compilers
Licensing API for Windows	AutoCAD	AutoCAD 2023, 2024
	C	Microsoft Visual Studio 2019, 2022
	Visual Basic .NET	Microsoft Visual Studio 2019, 2022
	C#	Microsoft Visual Studio 2019, 2022
	C++	Microsoft Visual Studio 2019, 2022 GCC
	Delphi	Delphi 12
	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
	C# - .NET	.NET 8, .NET 9
	Note: An application linked with libhasp_windows_bcc_vendorld.lib always requires Sentinel LDK RTE on the machine.	

API	Programming Language	Tested Compilers
Licensing API for macOS	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
	C	Clang 12.0.0 or later Xcode 12.0 or later
	C# - .NET	.NET 8, .NET 9
Licensing API for Linux	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
	C	GCC
	C++	GCC
	C# - .NET Core	.NET 8, .NET 9
Licensing API for Android	Java	Oracle JDK 1.8
License Generation API for Windows	C, C#, Visual Basic .NET	Microsoft Visual Studio 2019, 2022
	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
License Generation API for Linux	C	GCC

API	Programming Language	Tested Compilers
Activation Sample Calling Web Services for Windows	C	Microsoft Visual Studio 2019, 2022 You may need to convert the provided workspace for the VS version used.
	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17
Activation Sample Calling Web Services for macOS	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
Activation Sample Calling Web Services for Linux	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
Runtime Environment Installer	C	Microsoft Visual Studio 2019, 2022
	MSI	InstallShield 12 InstallShield 2013 or later
Admin API for Windows	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
	C, C#, C++, Visual Basic .NET	Microsoft Visual Studio 2019, 2022
	C# - .NET Standard	.NET 8, .NET 9
Admin API for Linux	C	GCC
	C# - .NET Standard	.NET 8, .NET 9

API	Programming Language	Tested Compilers
Admin API for macOS	C	Clang 12.0.0 or later Xcode 12.0 or later
	C# - .NET	.NET 8, .NET 9
Envelope .NET Runtime API	C#	Microsoft Visual Studio 2019, 2022
Java Envelope Configuration API	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
Licensing Rest API for Windows	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
Licensing Rest API for Linux	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21
Licensing Rest API for macOS	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17 Open JDK 21

Current Firmware Version

The table that follows indicates the firmware version on Sentinel HL keys when Sentinel LDK was released.

Sentinel LDK Version	Firmware Version on...		
	Sentinel HL (Driverless Configuration) Keys	Sentinel HL (HASP Configuration) Keys	(Legacy) Sentinel HASP Keys
8.5, 9.0, 10.0, 10.2	4.x Firmware keys: 4.60 or 4.70 4.x Firmware keys with microSD: 4.61 6.x Firmware keys: 6.09	4.x Firmware keys: 4.35 or 4.70 6.x Firmware keys: 6.09	3.25
8.2, 8.3, 8.4	4.x Firmware keys: 4.60 4.x Firmware keys with microSD: 4.61 6.x Firmware keys: 6.09	4.x Firmware keys: 4.35 6.x Firmware keys: 6.09	3.25
8.0	4.x Firmware keys: 4.60 4.x Firmware keys with microSD: 4.61 6.x Firmware keys: 6.08	4.x Firmware keys: 4.35 6.x Firmware keys: 6.08	3.25
7.8, 7.9, 7.10	4.54	4.33	3.25
7.6, 7.7	4.53	4.33	3.25
7.5	4.27	4.27	3.25

To determine the version of the firmware for any given Sentinel HL key, connect the key to a computer where Sentinel LDK RTE is installed. View the list of keys in Admin Control Center.

- > If the firmware version on a given Sentinel HL (HASP configuration) key is earlier than 4.60, the firmware is automatically upgraded when you upgrade the key to Sentinel HL (Driverless configuration). The firmware is upgraded to the latest version (based on the version of the License Generation libraries in use).

This upgrade affects the firmware only—Sentinel LDK functionality remains unchanged. This upgrade is not relevant for HL Drive microSD keys.

- > If the firmware on a Sentinel HL (Driverless configuration) key is earlier than 4.27, then the first time you assign concurrency to a license on the key, the firmware on the key is automatically upgraded to the latest version (based on the version of the License Generation libraries in use).

Documentation

This section describes the documentation provided with Sentinel LDK.

Online Documentation

Most Sentinel LDK documentation can be found online at:

[Sentinel LDK documentation](#)

Locally Installed Documentation

The Sentinel LDK documentation described below is placed on the local machine where Sentinel LDK is installed.

Software Protection and Licensing

Sentinel LDK documents can be found where Sentinel LDK is installed, under:

%ProgramFiles(x86)%\Thales\Sentinel LDK\Docs

Document	Description
Sentinel LDK with Sentinel LDK-EMS – Installation Guide	Details the prerequisites and procedures for installing Sentinel LDK Vendor Tools, Sentinel LDK-EMS Server (only for Sentinel LDK-EMS on-premises), launchers for Sentinel LDK-EMS, and the Run-time Environment.
Sentinel LDK Software Protection and Licensing Guide	Familiarize you with the Sentinel LDK applications and their functionality. This guide provides in-depth information about the logic of the applications and best practices for maximizing your software protection and licensing strategies. The guide describes a wide range of licensing strategies and models that you can implement, and can serve as the basis for elaboration and for creating new, tailor-made licensing models.
Sentinel LDK: Choosing and Integrating Hardware-, Software-, and Cloud Licensing	Provides a description of the differences and advantages of SL and cloud-based protection keys versus HL keys.

Tutorials and Quick Start Guides

Learn how to work with Sentinel LDK and familiarize yourself with the various components that let you protect and license your software. Get your free Sentinel LDK Demo Kit package or downloadable demo from your Thales sales representative

Document	Description
Sentinel LDK Software Protection and Licensing Tutorials	<p>Familiarize you with the Sentinel LDK applications and their functionality.</p> <ul style="list-style-type: none">> The Demo Kit tutorial is for vendors that want to evaluate Sentinel LDK.> The Starter Kit tutorial is for vendors that have already purchased Sentinel LDK. <p>Two versions of each tutorial are provided – one for working with Sentinel LDK-EMS as the back office system, and one for vendors who want to provide their own back office system and only use the Sentinel LDK APIs to handle licensing and protection.</p>
Sentinel LDK Quick Start Guide	Provide a short and simple demonstration of how you can easily protect your software using Sentinel HL keys.

Migration Guides

The following guides describe how to migrate to Sentinel LDK from earlier products.

Document	Description
Guides for Migrating to Sentinel LDK	<p>These guides describe how to migrate to Sentinel LDK from:</p> <ul style="list-style-type: none">> Hardlock> SmartKey> Sentinel SuperPro> HASP HL> HASP4> Sentinel Hardware Keys

Sentinel LDK-EMS

Sentinel LDK-EMS documents can be found where Sentinel LDK-EMS is installed, under:

%ProgramFiles(x86)%\Thales\Sentinel LDK-EMS\EMSServer\webapps\ems\Docs

Sentinel LDK-EMS Configuration Guide	Provides information on setting up and configuring Sentinel LDK-EMS to satisfy the requirements of your organization.
Sentinel LDK-EMS User Guide	Provides the Sentinel LDK-EMS user with detailed directions on how to set up license entities and how to handle entitlements, production, and support for Sentinel HL and SL keys. (This information is also provided in online help for the Sentinel LDK-EMS user interface.)
Sentinel LDK-EMS Web Services Guide	Provides the developer with an interface for integrating Sentinel LDK-EMS functionality into the vendor's existing back-office systems.
Integrating Sentinel LDK-EMS Server Into Your Existing Back-Office Systems	Outlines the many ways that software vendors can maximize the potential of their existing back-office systems, such as ERP, CRM, and business intelligence systems, through seamless integration with Sentinel LDK-EMS Server. This guide can be found where Sentinel LDK is installed, under: %ProgramFiles(x86)%\Thales\Sentinel LDK\Docs\

Getting Started Guides for Non-Windows Platforms

Getting Started Guides for Sentinel LDK under non-Windows operating systems can be found as follows:

Document	Location
Getting Started Guide for Linux	In the Linux download, or where Sentinel LDK is installed, under: %ProgramFiles(x86)%\Thales\Sentinel LDK\Additional Platforms\Linux\
Getting Started Guide for macOS	In the Mac download, or where Sentinel LDK is installed, under: %ProgramFiles(x86)%\Thales\Sentinel LDK\Additional Platforms\MacOS\
Getting Started Guide for Android	Where Sentinel LDK is installed, under: %ProgramFiles(x86)%\Thales\Sentinel LDK\Additional Platforms\Android\

Sentinel LDK and Sentinel LDK-EMS User Interfaces

The documentation described in the table that follows can be accessed from the user interface for the relevant Sentinel LDK component.

Document	Description
Sentinel Admin Control Center User Guide	Documentation for the end user, describing Sentinel Admin Control Center and providing instructions for performing the various functions such as updating or attaching licenses.
Sentinel LDK-EMS User Guide	Provides the Sentinel LDK-EMS user with detailed directions on how to set up license entities and how to handle entitlements, production, and support for Sentinel HL and SL keys.
Sentinel LDK Data Encryption Utility User Guide (Separate versions for Windows and for Mac)	Provides the developer with a description of the Sentinel LDK Data Encryption utility (formerly DataHASP utility), used for protecting data files that are accessed by Sentinel LDK Envelope.
Sentinel LDK Envelope User Guide (Separate versions for Windows, macOS, and Linux)	<p>Describes how to employ Sentinel LDK Envelope to automatically wrap your programs with a protective shield. The application provides advanced protection features to enhance the overall level of security of your software.</p> <p>The user guide for Linux can be found in the Linux download, or where Sentinel LDK is installed, under: %ProgramFiles (x86)%\Thales\Sentinel LDK\Additional Platforms\Linux\Docs\Manuals & Tutorials.</p>
Sentinel LDK ToolBox	Describes how to work with the ToolBox user interface for the Licensing API, License Generation API, and Admin API. Using Sentinel LDK ToolBox, the developer can experiment with the individual functions that are available in each API and can generate programming code for insertion in the developer's own program. Provides full documentation for each of the included APIs.

Sentinel LDK APIs

Documentation for the Sentinel LDK APIs described below can be found where Sentinel LDK is installed, under:
%ProgramFiles(x86)%\Thales\Sentinel LDK\API

Sentinel LDK API	Description
Admin API Reference	Provides the functionality available in Admin Control Center and Sentinel License Manager in the form of callable API functions.
Licensing API Reference (formerly Run-time API)	Provides the developer with an interface to use the licensing and protection functionality available in the Sentinel LDK Run-time Environment.
Run-time Installer API	Provides the developer with an interface for integrating installation of the Run-time Environment into the installation of the vendor's protected application.
License Generation API Reference	Provides access to the power and flexibility of Sentinel protection keys without the need to use Sentinel LDK-EMS. The developer can call functions in this API to generate and update licenses for Sentinel protection keys.

Resolved Issues

> ["Release: 10.2 " below](#)

Release: 10.2

The following issues that were reported by vendors were resolved in this release.

Reference	Resolved Issue	Component
SM-192364	Incorrect product names were shown in Admin Control Center when accessing remote licenses.	Run-time Environment
SM-197058	Station count-based concurrency does not work correctly in trusted storage environments when the client connects through a Remote Desktop session.	Run-time Environment
SM-178167	Protected applications built with Java, ScriptEnv, or LinuxEnv fail to launch on ARM 64 systems.	Envelope
SM-204685	Executable stack generated due to missing <code>GNU_STACK</code> segment.	Envelope
SM-204975	Timing in security checks causes startup issues in Java class-level protected applications.	Envelope-Java
SM-202714	Error message handling fails during initialization of .NET DLLs.	Envelope-.NET
SM-185043	Application fails to refresh when loading and protecting multiple .NET DLLs from a single project (.prjx).	Envelope-.NET
SM-197863	Runtime incompatibility occurs between Java class-level protection and Linux applications using GTK3.	Envelope-Java

Known Issues and Workarounds

The known issues in Sentinel LDK 10.2 that are likely to have the most significant impact on users are listed below, according to component.

Additional, less-common issues can be found [here](#).

In this section:

- > "Sentinel LDK Installation and Software Manager" below
- > "Sentinel LDK-EMS" on the next page
- > "End Users, Sentinel LDK Run-time Environment, License Manager, and Customer Tools" on page 39
- > "Sentinel LDK Envelope and Data Encryption for Windows Platforms" on page 41
- > "Sentinel LDK Envelope and Data Encryption for Linux" on page 45
- > "Sentinel LDK Envelope, Data Encryption, and Licensing API for macOS" on page 46

Sentinel LDK Installation and Software Manager

Ref	Issue
SM-35287	<p>When upgrading from Sentinel LDK v.7.3 through v.7.8 to Sentinel LDK v.7.10, all non-English locales of Customer contacts and Channel Partner contacts in Sentinel LDK-EMS are converted to the English locale.</p> <p>Note: You can ignore this issue if all of your Customer and Channel Partner contacts are set up to use the English locale or if you are not upgrading Sentinel LDK-EMS.</p> <p>Workaround: A solution for this issue is provided in the technical note available here.</p>
SM-109765	<p>Under Windows 11, notifications from Sentinel LDK regarding software updates are not being delivered to vendors by the software manager (Sentinel Up).</p> <p>Workaround: Monitor the Sentinel LDK download page and see when updates are published.</p> <p>You can also subscribe to this page (article KB0021845) to receive notifications: https://supportportal.gemalto.com/csm?id=kb_article_view&sys_kb_id=c2241c1d1bb41890f12064606e4bcb3e&sysparm_article=KB0021845</p>

Sentinel LDK-EMS

Ref	Issue
SM-12832	<p>When a user clicks the link provided in an email (that is sent by Sentinel LDK-EMS) to display a scheduled report, the report is not displayed when the DNS server cannot resolve the server hostname present in the link. Instead, the message "This page can't be displayed" is shown.</p> <p>Workaround: In the etc/host file on the user's machine, add an entry that contains the hostname and IP address of the Sentinel LDK-EMS machine.</p>
SM-19045	<p>Customers who were associated with a channel partner prior to Sentinel LDK 7.7 will not be visible in Sentinel LDK-EMS to the relevant Channel Partner user. However, the Channel Partner user will not be able create a new entry for an existing customer with the same email address as already exists in the EMS database. In this situation, the Channel Partner user will not be able to fulfill an entitlement for the customer.</p> <p>Workaround: If the Channel Partner user cannot create the required customer in Sentinel LDK-EMS, the software vendor should handle the fulfillment of the entitlement for the customer.</p>
SM-108638	<p>After you upgrade to the latest version of Google Chrome or to Microsoft Edge version 95 or later, functionality related to protection keys is blocked if you access Sentinel LDK-EMS using HTTP mode. This applies to both the vendor portal and the customer portal.</p> <p>Workaround: Switch Sentinel LDK-EMS to HTTPS mode.</p>
SM-52262	<p>After you introduce or update a Master Key, you must notify all Sentinel LDK-EMS users to log off and log on again to get the latest changes.</p>
SM-68428	<p>When you generate a product key entitlement in Sentinel LDK-EMS, the customer does not receive the entitlement certificate email if the customer contact locale is not specified.</p> <p>Workaround: Specify the locale for the customer.</p>
SM-139221	<p>Producing a re-opened entitlement results in the following error:</p> <p>"An internal error occurred. Contact the system administrator for assistance. "</p> <p>This issue occurs after an entitlement was re-opened.</p> <p>Workaround: Do not reopen an entitlement if there are already any activations for the entitlement. You can copy the entitlement if you want to create a new entitlement.</p>

End Users, Sentinel LDK Run-time Environment, License Manager, and Customer Tools

Ref	Issue
	<p>The Sentinel Remote Update System (RUS utility) is not supported for Mac systems.</p> <p>Workaround: To obtain a fingerprint, use Sentinel Admin Control Center.</p>
SM-116811	<p>When installing a different version of Sentinel LDK Run-time Environment (RTE) over an existing version on a Linux platform, the newly-installed hasplmd daemon is typically started automatically. However, in the following instances, the hasplmd daemon is not started automatically:</p> <ul style="list-style-type: none"> > When upgrading RTE version 8.13 or earlier to RTE version 8.15 or later <p>OR</p> <ul style="list-style-type: none"> > When downgrading RTE version 8.15 or later to RTE version 8.13 or earlier <p>Workaround: After installing the desired version of the RTE, do either of the following:</p> <ul style="list-style-type: none"> > Install the desired version of the RTE a second time. After performing the second installation, the hasplmd daemon starts automatically. <p>OR</p> <ul style="list-style-type: none"> > Start the hasplmd daemon manually by entering the command: systemctl start hasplmd
SM-94994	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> > An RTE without legacy drivers is installed on a new machine. > An RTE with legacy drivers is installed afterward on the machine. <p>An application that requires an RTE with legacy drivers will not operate successfully. During installation of the RTE with legacy drivers, no warning or error is generated.</p> <p>Workaround: Using Admin Control Center, generate a diagnostic report, and contact Thales Technical Support.</p>
SM-82475	<p>Given the following situation:</p> <ul style="list-style-type: none"> > When the current state of an SL key is decoded (using SL License Generation API), the status of the container is shown as Secure Storage Id Mismatch in the Key ID column. > The key contains a Product that is rehostable or detachable OR the Product license type is Executions or Expiration Date. <p>If the SSID (secure storage ID) of the container changes (for example, the container becomes corrupted or is deleted), the Product will be marked as Cloned and become unusable. In any other situation, the status Secure Storage Id Mismatch has no significance and can be ignored.</p>

Ref	Issue
SM-76660	<p>Given the following circumstances:</p> <ol style="list-style-type: none"> 1. Windows is installed on a Mac machine with Boot Camp. 2. An SL license is installed in the Windows system. <p>The Secure Storage ID may change and cause Feature ID 0 to be flagged as "cloned".</p> <p>Workaround: Do not install the SL license in the Windows system. Have your application consume a network seat from a cloud license.</p>
SM-70131	<p>The Sentinel LDK License Manager (process hasplms.exe) hangs intermittently and reaches a very high CPU utilization (approximately 1.9 GB).</p> <p>Workaround: Protect the application using the latest API libraries and, if the RTE is required on the end user's machine, upgrade to the most recent RTE.</p>
SM-59868	<p>An application linked with libhasp_windows_bcc_vendorld.lib requires Sentinel LDK Run-time Environment on the machine.</p>
SM-546	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> > A protected application was created using Visual Studio 2015 > Control Flow Guard is explicitly enabled in Visual Studio. > The application links statically or dynamically with Sentinel Licensing API. > The External License Manager (hasp_rt.exe) is not used. > The application is run under Windows 10, or Windows 8.1 Update (KB3000850). (Not all Windows 8.1, only recent ones) <p>The protected application may fail.</p> <p>Workaround: Include the External License Manager (hasp_rt.exe) with the protected application.</p>
LDK-14971	<p>Given the following circumstances at a customer site:</p> <ul style="list-style-type: none"> > One machine has Run-time Environment version 7.51. > A second machine has a version of Run-time Environment that is earlier than v.7.51. > The customer performs rehost of a license repeatedly between the two machines. > An update is applied to the license on either of these machines. <p>A rehost operation may fail with the message HASP_REHOST_ALREADY_APPLIED.</p> <p>Workaround: Obtain a new SL license from the software vendor for the protected application on the target machine. Before attempting any additional rehost procedure, install the latest Run-time Environment on both machines.</p>

Ref	Issue
LDK-12547	<p>Under Linux, if the user is running a Windows 64-bit protected application using Wine with default options, Linux may return a "debugger detected" error.</p> <p>Workaround: When you protect the application using Envelope, disable User debugger detection for the application. (Note that disabling debugger detection reduces the overall security of the application.)</p>
LDK-10670	<p>After a user connects a Razer Abyssus mouse and installs Razer drivers on a computer, the device manager on the computer does not recognize a Sentinel HL key if the key is connected to the same USB port where the mouse was previously connected.</p> <p>This issue has been reported to Razer.</p>
LDK-9044	<p>Given the following circumstances:</p> <p style="padding-left: 40px;">A Sentinel HL (Driverless configuration) key is connected to a USB host controller in default mode on QEMU emulator version 2.0.0 and Virtual Machine Manager version 0.9.5.</p> <p>When the key is disconnected, the key continues to be displayed in Admin Control Center as a connected key. (However, a protected application whose license is located in the key does not execute after the key is disconnected.)</p> <p>Workaround: Switch the USB controller to USB 2.0 mode.</p>
LDK-8480	<p>With some new USB chipsets, it is possible that the hasp_update() API call, used to update the firmware of Sentinel HL keys to version 3.25, will generate the HASP_BROKEN_SESSION return code, even if the firmware is correctly updated. (This issue does not occur with Sentinel HL Driverless keys with firmware version 4.x.)</p> <p>Workaround: Install the latest Run-time Environment. The automatic firmware update feature of the License Manager will automatically update the firmware of the key the first time that the key is connected, without the need to call hasp_update().</p>

Sentinel LDK Envelope and Data Encryption for Windows Platforms

General

Ref	Issue
LDK-11727	<p>Debugger detection is not provided for .NET applications.</p> <p>Workaround: Implement debugger detection mechanism in the application code, and use Envelope to protect the methods that call these functions.</p>

Ref	Issue
LDK-11191	When a protected application is run under Novell ZENworks Agent, the application may generate "Debugger Detected" errors and may fail to run. This is because ZENworks Agent attaches to the started application as a debugger in order to monitor different events.
LDK-6695	When a "Debugger Detected" error is generated, it is not possible for the protected application to determine which process is regarded as a debugger.
LDK-8850	When a protected application detects that a debugger is attached, the application may generate multiple "Debugger Detected" message windows.
SM-58676	<p>Given the following circumstances:</p> <ol style="list-style-type: none"> 1. Install SL AdminMode licenses on your local machine. 2. Run IObit Advanced SystemCare Ultimate 12 to clean and optimize your machine. 3. Restart your machine. <p>Local SL AdminMode licenses may be missing or may be identified as cloned licenses. This is an issue with the IObit product. Thales has reported this issue to IObit and it is currently under investigation.</p> <p>Workaround: Do not use the current version of the IObit product, <i>OR</i> do not use SL AdminMode licenses until this issue is resolved. (You can use SL UserMode licenses.)</p>
SM-65381	<p>Under Windows, execution of a Python application that is protected with DFP sometimes fails with the "Bad magic number" error if hasp_rt.exe is not present in the protected folder.</p> <p>Workaround: Ensure that hasp_rt.exe is present in the protected folder.</p>
SM-171160	<p>[User-Based Licensing] An application protected with Envelope cannot continue to run if you disassociate the product from the user and re-associate the product with a user in Sentinel EMS during the execution of the protected application.</p> <p>Workaround: Exit the application and launch the application again.</p>

Java

Ref	Issue
LDK-11195	<p>When protecting a Java application, Envelope fails with the message "Serious Internal Error (12)".</p> <p>Workaround: If this error occurs, protect the Java application using either of the following techniques:</p> <ul style="list-style-type: none"> > If the application contains JARs within a JAR/WAR executable, remove those JARs when protecting the executable with Envelope. You can add the JARs to the JAR/WAR executable after protection is complete. > Create a JAR/WAR executable using only those classes that you want to protect. After applying protection, you can add other classes or JARs, or any other dependencies in the protected JAR/WAR executable.
SM-10890	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> > An Envelope project was created with Envelope version 7.3 or earlier. > The project contains settings for a Java application. > On the Protection Settings tabbed page for the Java application, you select the option to overwrite default protection settings. <p>The Allows grace period after failed license check check box should be modifiable. However, the check box cannot be changed.</p> <p>Workaround: On the Advanced tabbed page, make any change to the MESSAGE_OUTPUT_MODE property, and then change it back. This forces Envelope to load an internal data structure that then makes the Allows grace period after failed license check check box modifiable.</p> <p>Note: This grace period is not supported for Web applications.</p>
SM-10969	<p>Due to a known limitation in Java, if a background check thread becomes non-EDT, the background check (Abort/Retry/Ignore) dialog box may not appear. Envelope has been modified so that the error dialog prompted by the protected method in the protected application takes precedence. This has reduced the occurrence of the problem, but it has not eliminated the problem entirely.</p>
SM-98384	<p>A protected WAR does not run successfully on WildFly Server 23.</p>
SM-110174	<p>Java class level protection and Data File protection in Windows Envelope for 64-bit applications are not supported under Wine.</p>

.NET

Ref	Issue
SM-554	<p>For apps that target the .NET Framework version 4.6 and later, CultureInfo.CurrentCulture and CultureInfo.CurrentUICulture are stored in a thread's ExecutionContext, which flows across asynchronous operations. As a result, changes to the CultureInfo.CurrentCulture and CultureInfo.CurrentUICulture properties are reflected in asynchronous tasks that are launched subsequently.</p> <p>If the current culture or current UI culture differs from the system culture, the current culture crosses thread boundaries and becomes the current culture of the thread pool thread that is executing an asynchronous operation.</p> <p>When protecting a sample application implementing above behavior with protection type as "Dot Net Only", then the application behaves as expected. However, with protection type "Dot Net and Windows Shell" or "Windows Shell Only", the thread uses the system's culture to define behavior.</p> <p>Workaround:</p> <p>Do the following:</p> <ol style="list-style-type: none"> 1. Use .NET Framework 4.5. 2. Use <pre>CultureInfo.DefaultThreadCurrentCulture = new CultureInfo(...)</pre> instead of <pre>Thread.CurrentThread.CurrentCulture = new CultureInfo(...).</pre>
SM-25875	<p>Given the following circumstances:</p> <ol style="list-style-type: none"> 1. A .NET application is protected with Envelope. 2. The protection type includes Windows Shell (with or without the method level). 3. The application attempts to get a module handle using the following method: <pre>IntPtr hMod = Marshal.GetHINSTANCE(Assembly.GetExecutingAssembly() .GetModules()[0])</pre> <p>The handle returned may not be correct, and as a result, an error will be generated.</p> <p>Workaround: You can call the GetModuleHandle system API of the Kernel32.dll to get the module handle.</p> <p>For example:</p> <pre>[DllImport("kernel32.dll", CallingConvention = CallingConvention.StdCall, CharSet = CharSet.Auto)] private static extern IntPtr GetModuleHandle(IntPtr lpModuleName); IntPtr hMod = GetModuleHandle(Process.GetCurrentProcess().MainModule.ModuleName);</pre>

Ref	Issue
SM-26578	<p>If a .NET application protected with Windows Shell sets the exit code to ExitEventArgs such as "e.ApplicationExitCode = 1" when the application exits, the exit code cannot be retrieved by an external process.</p> <p>Workaround: Call "Environment.Exit(1)" to exit the process.</p>

Sentinel LDK Envelope and Data Encryption for Linux

Ref	Issue
SM-28403	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> > A Linux application is protected with Envelope, with protection against debugging. > The application calls the wait(&status) system call. This is equivalent to: <pre>waitpid(-1, &status, 0)</pre> <p>The application may hang.</p> <p>Workaround 1: Call waitpid for a specific child process pid (pid > 0).</p> <p>Workaround 2: Disable the anti-debugging feature in Envelope. Note: This workaround significantly reduces the security of the protected application. Thales recommends that you consult with Technical Support before choosing this workaround.</p>
SM-69080	<p>A protected application may not handle signals properly when:</p> <ul style="list-style-type: none"> > Background check is enabled, and > Signal handlers are registered by a thread created by the application. <p>Workaround: Do one of the following:</p> <ul style="list-style-type: none"> > Disable both background check and anti-debugging. (You can do this by specifying the following line command flags: <code>-b:0 --debug --memdump</code>) > (Preferred workaround) Register the signal handler in a main thread instead of a thread function. Thread function is one of the following: <ul style="list-style-type: none"> • A function passed to pthread_create as start_routine • A function called from start_routine.

Sentinel LDK Envelope, Data Encryption, and Licensing API for macOS

Ref	Issue
LDK-11655	<ul style="list-style-type: none">> When running Envelope in a VMware Fusion 7.1.1 virtual machine on a Mac machine, if you save the protected application to an HGFS (Host Guest File System) volume, the application file is corrupted.> When you run a protected application on a VMware Fusion virtual machine from an HGFS share, if the application requires write access, the error "unable to write to file" is generated.
SM-57838	The command line Envelope tool (envelope_darwin) now only works if Envelope.app (UI bundle) is in the same folder. To use the command line tool, copy Envelope.app to the folder that contains the command line tool.
SM-57024	Dark Mode has been introduced by Apple in macOS 10.14 but is not supported yet by the Envelope GUI. You should disable Dark Mode to have a proper user experience.
SM-51456	<p>Due to reliability enhancements in Sentinel LDK under macOS, there is some performance impact in protected applications under macOS 10.13.</p> <p>A technical note will be issued that describes this issue and the option to disable these enhancements in favor of higher performance.</p>