Sentinel LDK 8.4 with Sentinel LDK-EMS

RELEASE NOTES

Revision History

Part number 007-000667-003, Revision A, 2204-1

Disclaimer and Copyrights

CONTENTS

Sentinel LDK 8.4 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 this location:

https://docs.sentinel.thalesgroup.com/ldk/home.htm

Release: **8.4** | April 2022

Product Overview

Sentinel LDK is Thales's 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: 8.4 " below

> **NOTE**   If you are upgrading from a version of Sentinel LDK that is earlier than 8.3, be sure to review the release notes for all intervening versions. Significant enhancements and changes are introduced in each version of Sentinel LDK. You can download a zip file that contains all Sentinel LDK release notes.

Release: **8.4**

In this section:

> "Support for Active-Active High Availability for Cloud Licensing" below

> "Dynamic Memory is Now Supported for SL Keys" on the next page

> "Default Locking Type Changed to "HL or SL (AdminMode or UserMode)"" on the next page

> "Locking Type Can Now Be Modified in the Catalog for Deployed or Queued Products" on the next page

> "Client Identities Can Now Be Assigned an Expiration Date" on the next page

> "Licensing API Can Now Reserve and Release Executions" on page 9

> "Enhancements and Changes to Sentinel LDK Envelope" on page 9

> "Hardlock.sys has been Removed from the RTE Installer" on page 10

> "Sentinel LDK-EMS Now Uses Tomcat Version 9.0.56" on page 10

> "Sentinel LDK-EMS Web Services Now Return eid and createdBy in Response Body" on page 10

> "Sentinel LDK-EMS No Longer Generates an RTE Installer" on page 10

Support for Active-Active High Availability for Cloud Licensing

Sentinel LDK now supports configuring a vendor-hosted cloud license server for high availability.

Sentinel LDK License Managers in the vendor's data center can be configured to store licenses in a common external trusted license storage (a MySQL database cluster).

You can set up License Managers on two or more active license server machines. A load balancer will distribute license requests between the machines and will maintain access to licenses in case a server becomes unavailable.

For information on setting up high availability for cloud licensing, see the Sentinel LDK High Availability for Cloud Licensing Configuration Guide.

Dynamic Memory is Now Supported for SL Keys

Until now, dynamic memory was supported only for Products that are licensed using HL keys (excluding Basic and Pro keys). Now, dynamic memory is supported for Products that are licensed with SL AdminMode and SL UserMode keys. (Dynamic memory is not supported for SL Legacy keys.)

For SL AdminMode keys, Sentinel Run-time Environment 8.41 or later is required.

Default Locking Type Changed to "HL or SL (AdminMode or UserMode)"

When defining a new Product in the Sentinel LDK-EMS Catalog, the default locking type is now **HL or SL (AdminMode or UserMode)** instead of **HL**. This change has no effect on existing Products.

Locking Type Can Now Be Modified in the Catalog for Deployed or Queued Products

Previously, once a Product in the Sentinel LDK-EMS was deployed or queued, it was no longer possible to change the locking type for the Product in the Catalog. Now, you can now modify the locking type in the Catalog for deployed or queued Products as follows:

Current Locking Type	Modified Locking Type
HL	HL or SL AdminMode, OR HL or SL (AdminMode or UserMode)
SL AdminMode	HL or SL AdminMode, OR HL or SL (AdminMode or UserMode)
SL UserMode	HL or SL (AdminMode or UserMode)

When changing from the HL locking type to a locking type that includes SL, the **Clone Protection** and the **Rehost** parameters in the Features also become available for configuration.

> **NOTE** Any changes to Products or Features in the Catalog have no effect on deployed or queued Products.

Client Identities Can Now Be Assigned an Expiration Date

You can now set an expiration date for client identities. This enables you to:

> Easily manage trials by providing users with expiring identities that consume the same license. This removes the need to generate a new key and a new license for each trial.

> Manage which users can access a concurrency license and for how long.

Licensing API Can Now Reserve and Release Executions

For Features that are licensed with the **Execution Count** license type, the application can now reserve a specific number of executions when it logs in to the protection key (using the LoginScope function in Sentinel Licensing API). If any of the reserved executions are not consumed by the application, they are returned to the pool of executions in the license when the application logs out of the protection key.

This ensures that the application has access to enough executions before it starts to use the licensed Feature.

This functionality is only available with SL keys and is only applicable when using C-language function calls. The function requires Run-time Environment 8.41 or later.

Enhancements and Changes to Sentinel LDK Envelope

Sentinel LDK Envelope has been enhanced or modified as follows:

> When an unexpected error occurs during protection of a file, Envelope now displays a message and provides a link that simplified reporting the issue. This should improve the response time for obtaining assistance from Thales to resolve this type of issue.

> The user interface for working with AppOnChip has been improved.

> The WinV3 protection engine now supports the advanced debugger detection feature.

> Envelope for Linux now displays a warning message when the --debug option is used when also selecting --memdump.

> The behavior of Envelope for Linux has been modified for debug and memdump parameters as follows:

Given that the following protection parameters are specified for an Envelope project:

- Debugging is allowed for the protected application. (The debug parameter was specified.)

- Memory dumps are not allowed for the protected application. (The memdump parameter was not specified.)

The behavior of Envelope is as follows:

- Version 8.3 and earlier: Both debugging and memory dumps are not allowed. No message is issued.

- Version 8.4 and later: Both debugging and memory dumps are allowed. A message regarding this situation is issued.

The reason for this behavior is that protection against memory dumps does not work when debugging of the protected application is enabled.

> Sentinel LDK Envelope for Android has been discontinued.

   The following Sentinel LDK functionality is no longer supported for native Android applications.

   • Sentinel LDK Envelope

   • Data file protection

   You can continue to use Sentinel Licensing API to protect native Android applications.

   If you require a protection solution for Android native libraries, contact Thales customer support.

Hardlock.sys has been Removed from the RTE Installer

The legacy Hardlock driver (hardlock.sys) is no longer installed as part of the Run-time Environment. RTE 8.31 is the last version that supports the legacy Hardlock driver.

The Hardlock driver is required when an application is licensed using a Hardlock parallel port key or a Hardlock USB key with a very old Hardlock library. In these situations, you must install RTE 8.31 or earlier. RTE 8.31 is available from Knowledgebase article KB0025777.

Starting with RTE 8.41, Hardlock LPT keys are no longer supported. Applications that use Hardlock USB keys need to be built with LDK API 6.4 or later. If an older version of the RTE is required, contact Thales customer support.

Sentinel LDK-EMS Now Uses Tomcat Version 9.0.56

The installation and upgrade procedures for Sentinel LDK-EMS (On-Premises) now install Tomcat version 9.0.56.

Sentinel LDK-EMS Web Services Now Return eid and createdBy in Response Body

When you search for an entitlement using `<version>/ws/entitlement.ws` or `<version>/ws/entitlement/{entId}.ws`, the response body now automatically includes the eid and createdBy values in addition to any query parameters.

Sentinel LDK-EMS No Longer Generates an RTE Installer

The **Developer > RTE Installer** tab has been removed from Sentinel LDK-EMS. You can generate a customized Run-time Environment (RTE) installer using the Sentinel LDK Master Wizard.

> For details on generating a Run-time Environment installer that is customized with your Vendor Codes, see Sentinel LDK Installation Guide.

> For details on signing a Run-time Environment installer, see Sentinel LDK Software Protection and Licensing Guide.

Installation and Upgrades

Visit the Sentinel LDK download page for the most recent versions of Sentinel LDK software and embedded documentation.

Release: **8.4**

In this section:

Installing Linux and Mac Packages

Sentinel LDK files required for Linux and Mac platforms 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 the relevant packages directly from the Thales website:

> Linux: https://supportportal.thalesgroup.com/csm?id=kb_article_view&sys_kb_
id=1d6107451b05d050f12064606e4bcbb0&sysparm_article=KB0021880

> Mac: https://supportportal.thalesgroup.com/csm?id=kb_article_view&sys_kb_
id=fc624f891b05d050f12064606e4bcb4e&sysparm_article=KB0021881

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 8.4 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 8.4.

> **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 8.4 has been tested only for Sentinel LDK v.8.0 and later.

If you plan to upgrade from an earlier version of Sentinel LDK, please 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

Release: **8.4**

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.

Release: **8.4**

In this section:

Sentinel LDK Run-time Environment and Protected Applications for End Users

Sentinel LDK Run-Time Environment version 8.41 is provided for Windows, Mac, and Linux (Intel and ARM) systems.

To support all of the latest enhancements in Sentinel LDK, and to provide the best security and reliability, end users should receive the latest Run-time Environment (*RTE*).

> **NOTE**
>
> > When working with 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.)
>
> > 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.

For all pre-existing functionality in Sentinel LDK, earlier versions of the RTE are supported as follows:

> **When using customized vendor API libraries v.8.41 - version-restricted option:**

Whenever the RTE is required, Sentinel LDK RTE v.8.15 or later must be provided.

> **When using customized vendor API libraries v.8.41 - version-unrestricted option:**

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 RTE, and protected applications (with or without the RTE), can be installed under the following systems:

System	Supported Versions
.NET	Sentinel LDK provides support for the following target frameworks: > .NET Framework: v2.0 - v4.8 > .NET Standard: v2.1 > .NET Core: v2.1, v3.1 > .NET 5: v5.0 > .NET 6: v6.0 Protected applications that use the supported .NET frameworks are supported on the following platforms: > Windows (Win32 and x64) > Linux Intel (x86_64) > Linux ARMHF > Linux ARM64 > Mac (only protected with Licensing API) **NOTE** When protected with Envelope: .NET Core applications with platform-specific functionality such as Windows Forms and Windows Presentation Foundation (WPF) work only on Windows platforms.
Windows	x86 and x64 versions of the following: > Windows Server 2012 R2 > Windows Server 2016 > Windows Server 2019 > Windows Server 2022 > Windows 10 IoT Enterprise 2019 LTSC > Windows 10 21H2 > Windows 11 **Note:** Windows Insider Preview builds are not supported. The latest service packs and security updates must be installed.
Mac	> macOS 10.15 Catalina > macOS 11.5 Big Sur > macOS 12.0 Monterey **Note:** The Sentinel Remote Update System (RUS utility) is not supported for Mac systems in this release. To obtain a fingerprint, use Sentinel Admin Control Center.

System	Supported Versions	
Linux	**Linux Intel (x86-64)**	> OpenSUSE Leap 15.3 > Red Hat EL 8.5 > Ubuntu Server 20.04 > Ubuntu Desktop 20.04 > Debian 11 > CentOS 8.4 The latest service packs and security updates must be installed.
	Linux ARM 32-bit (armel and armhf)	The following hardware/boards have been validated: > BeagleBone Black > Raspberry Pi-4 > NI cRIO-9068
	Linux ARM 64-bit (arm64)	The following hardware/board has been validated: > Qualcomm DragonBoard 410c
	Wine	Sentinel LDK RTE was tested on Linux platforms with Wine 7.0
Android	**Android ARM (64-bit)**	Android 10.x, 11.x, 12.x
	Android Architecture	The following architectures are supported: > armv7 > armv7a > arm64
	Android ABI	Sentinel LDK supports Android applications designed for the following Android application binary interfaces: > armeabi > armeabi-v7a > arm64-v8a

System	Supported Versions
Virtual Machines	The VM detection and VM fingerprinting capabilities provided by Sentinel LDK have been validated on the following technologies: > Parallels Desktop 17 for Mac > VMware Workstation 16 > VMware ESXi 6.7, 7.0 > Hyper-V Server 2019 (SL only) > Xen Project 4.15 > KVM (RHEL 8.5, Ubuntu 20.04 server, Debian 11) > Microsoft Azure > VirtualBox 6.1.x > Docker (Linux) containers, including under Kubernetes > LXC containers

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	x64 versions of the following: > Windows Server 2016 > Windows Server 2019 > Windows Server 2022 > Windows 10 21H2 > Windows 11 21H2 **Note:** Windows Insider Preview builds are not supported. The latest service packs and security updates must be installed.

Sentinel LDK-EMS Database

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

System	Supported Database Server Software
Windows	> Microsoft SQL Server 2016 > Microsoft SQL Server 2017 Express > Microsoft SQL Server 2019 Express **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.

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**: 9.0.56

> **JRE:** OpenJDK 8.232

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	x64 versions of the following: > Windows Server 2016 > Windows Server 2019 > Windows Server 2022 > Windows 10 21H2 > Windows 11 21H2 **Note:** Windows Insider Preview builds are not supported. The latest service packs and security updates must be installed. **Display:** Requires a minimum screen resolution of 1280 by 1024 pixels with 24-bit color quality. **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.
Mac	> macOS 11.5 Big Sur > macOS 12.0 Monterey Applications built on the Cocoa framework are supported. **Web Browsers for Sentinel Vendor Tools Help Systems:** > Mozilla Firefox > Mac Safari with configuration option **Cross-Origin Restriction** disabled. (This option can be accessed from the **Developer** menu.)

System	Supported Versions
Linux Intel	Sentinel LDK Envelope for Linux and Master Wizard for Linux are supported on the x86-64 version of the following distributions of Linux: > OpenSUSE Leap 15.3 > Red Hat EL 8.5 > Ubuntu Server 20.04 > Ubuntu Desktop 20.04 > Debian 11 > CentOS 8.4 The latest service packs and security updates must be installed.
Linux ARM	> ARM 32-bit > ARM 64-bit 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.
Android	Android ARM platforms
Java	Java 8

Vendor Library Version Dependency

Your customized Vendor libraries (**haspvlib_<vendorID>.***) are downloaded each time that you introduce your vendor keys to Sentinel LDK. You should re-introduce 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 be equal to or later than the version of the customized Vendor library. For example:

Vendor Library Version	Required Run-time Environment Version
7.100	7.100 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

Vendor Library Version	Required Run-time Environment Version
8.23	8.23 or later
8.31, 8.32, 8.34	8.31 or later
8.41	8.41 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

> **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.

Supported Platforms for Code Samples

The code samples are supported on the same platforms as listed for "Sentinel LDK Vendor Tools " on page 20.

> **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 2020, 2021, 2022
	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 XE3
	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17
	C# - .NET Core	.NET Core 3.1
	C# - .NET	.NET 6
	Note: An application linked with **libhasp_windows_bcc_vendorId.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 OpenJDK 17
	C	Clang 12.0.0 or later Xcode 12.0 or later
	C# - .NET	.NET 6
Licensing API for Linux	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17
	C	GCC
	C++	GCC
	C# - .NET Core	.NET Core 3.1 .NET 6
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 OpenJDK 17
License Generation API for Linux	C	GCC
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 OpenJDK 17

API	Programming Language	Tested Compilers
Activation Sample Calling Web Services for macOS	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17
Activation Sample Calling Web Services for Linux	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17
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 OpenJDK 17
	C, C#, C++, Visual Basic .NET	Microsoft Visual Studio 2019, 2022
Admin API for Linux	C	GCC
Admin API for macOS	C	Clang 12.0.0 or later Xcode 12.0 or later
Envelope .NET Runtime API	C#	Microsoft Visual Studio 2019, 2022
Java Envelope Configuration API	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17

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
8.2, 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).

Dropped Support

This section lists platforms and compilers that were supported in the past, but have not been tested with (or are no longer supported by) Sentinel LDK 8.4. Thales will continue to accept queries for issues related to these platforms and compilers, and will attempt to provide information to resolve related issues.

Dropped Support for Android applications in Sentinel LDK Envelope

Sentinel LDK Envelope no longer supports native Android applications. You can continue to use Sentinel Licensing API to protect these applications.

If you require a protection solution for Android native libraries, contact Thales customer support.

Platforms for Protected Applications for End Users

Support for the following platform has been discontinued for protected applications:

> Windows 8.1 SP1

Documentation

In this section:

Online Documentation

Most Sentinel LDK documentation can be found online at:

https://docs.sentinel.thalesgroup.com/ldk/home.htm

Locally Installed Documentation

Sentinel LDK documents can be found:

> where Sentinel LDK is installed, under:
   %ProgramFiles(x86)%\Thales\Sentinel LDK\Docs

> where Sentinel LDK-EMS is installed, under:
   %ProgramFiles(x86)%\Thales\Sentinel LDK-EMS\EMSServer\webapps\ems\Docs

Document	Description
Sentinel LDK 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.

Document	Description
Sentinel LDK Software Protection and Licensing Guide	Provides in-depth information about the logic of the applications and best practices for maximizing your software protection and licensing strategies. 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 Software Protection and Licensing Tutorials	Familiarize you with the Sentinel LDK applications and their functionality. > 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. 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.
Sentinel LDK High Availability for Cloud Licensing Configuration Guide	Describes how to set up "high availability" support to serve cloud-based licensing.
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.
Sentinel LDK Quick Start Guides	Provide a short and simple demonstration of how you can easily protect your software using Sentinel HL keys. Separate Demo Kit and Starter Kit guides are provided.
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.)

Document	Description
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.

Getting Started Guides

Getting Started Guides for other operating systems can be found as follows:

Linux

The *Getting Started 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**

macOS

The *Getting Started Guide for macOS* can be found in the Mac download or where Sentinel LDK is installed, under: **%ProgramFiles(x86)%\Thales\Sentinel LDK\Additional Platforms\MacOS**

Android

The *Getting Started Guide for Android* can be found 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.

Reference Document	Description
Sentinel Admin Control Center	Documentation for the end user, describing the Admin Control Center and providing instructions for performing the various functions such as updating or attaching licenses.

Reference Document	Description
Sentinel LDK-EMS	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 (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 (Separate versions for Windows and for Mac)	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.
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:

> On the Sentinel Product Documentation web site:

   https://docs.sentinel.thalesgroup.com/ldk/home.htm

> where Sentinel LDK is installed, under:
   %ProgramFiles(x86)%\Thales\Sentinel LDK\API

Sentinel LDK API	Description
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.

Sentinel LDK API	Description
Sentinel LDK-EMS Web Services	Provides the developer with an interface for integrating Sentinel LDK-EMS functionality into the vendor's existing back-office systems. Locally-installed documentation is available from the **index.html** menu under: **%ProgramFiles(x86)%\Thales\Sentinel LDK-EMS\EMSServer\webapps\ems\Docs**
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.
Admin API Reference	Provides the functionality available in Admin Control Center and Sentinel License Manager in the form of callable API functions.

Resolved Issues

Release: **8.4**

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

Reference	Resolved Issue	Components
SM-114671	Sentinel LDK Developer key was not recognized by Envelope engines (.Net, Java, WinNG).	Envelope-Win, .NET, Java, NG
SM-114470	Chinese characters were garbled in an Envelope error message.	Envelope-Win,.NET
SM-114462	.NET Envelope would fail to protect certain DLLs.	Envelope-.NET
SM-114908	.NET Envelope: Invalid VAR opcode: Idelem msg on terminal .	Envelope-.NET
SM-112663	Envelope cannot open project file under a Chinese version of Windows after the Chinese language pack is installed.	Envelope-GUI-Win
SM-112703	Envelope would fail when adding a .NET Core application with dependencies that use a lower version than exist in the project.	Envelope-.NET
SM-112829	A debugging log would be included in envelope.com during protection of a .NET application.	Envelope-.NET
SM-111408	Under poor network conditions, an Envelope grace message is not shown when expected.	Envelope-.NG
SM-118496	Under certain circumstances, when adding a DLL assembly to Envelope, an unsupported .NET assembly error (2012) is generated.	Envelope-.NET
SM-113922	Under certain circumstances, using Web Services to perform a product key update would fail with the following message: 400 Bad Request The input XML is not valid. Node - com.sfnt.ems.domain.ProductKey.	Sentinel LDK-EMS Web Services
SM-114383	After disabling an entitlement in the Entitlement table, there was no visible indication that the entitlement was disabled.	Sentinel LDK-EMS

Reference	Resolved Issue	Components
SM-111256	After you upgraded to the latest version of Google Chrome or to Microsoft Edge version 95 or later, functionality related to protection keys was blocked if you accessed Sentinel LDK-EMS using HTTP mode. This applied to both the vendor portal and the customer portal.	Sentinel LDK-EMS
SM-119586	After connecting to a VPN, when you click **Submit** on the Access to Remote ACC panel, a false-positive warning similar to the following was sometimes displayed: "A duplicate License Manager ID exists on this server and on the server at address 10.42.49.253. This is typically caused by cloning a VM. Licenses on these two servers may be inaccessible"	Sentinel License Manager
SM-119327	If no host is specified, AdminAPI uses "localhost" to connect to the License Manager. But in modern machines, localhost is resolved to "::1". This may not work because the IPv6 option may be disabled in the License Manager. AdminAPI now uses "127.0.0.1" instead of "::1".	Sentinel Admin API
SM-115393	When the client identity is installed in Admin Control Center, and the License Manger received a detached license from a remote machine, a local API was affected by the local License Manager detachable configuration. However, the local License Manager should have only acted as the forwarder in this case.	Sentinel License Manager

Known Issues and Workarounds

The known issues in Sentinel LDK 8.4 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 the next page

> "Sentinel LDK Envelope and Data Encryption for Windows Platforms" on page 39

> "Sentinel LDK Envelope and Data Encryption for Linux" on page 43

> "Sentinel LDK Envelope, Data Encryption, and Licensing API for macOS" on page 44

Sentinel LDK Installation and Software Manager

Ref	Issue
SM-35287	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. **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. **Workaround:** A solution for this issue is provided in the technical note available here.
SM-109765	Under Windows 11, notifications from Sentinel LDK regarding software updates are not being delivered to vendors by the software manager (Sentinel Up). **Workaround:** Monitor the Sentinel LDK download page and see when updates are published. 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

Sentinel LDK-EMS

Ref	Issue
SM-119258	Sentinel LDK-EMS Web Services does not support adding dynamic memory files to Products. **Workaround**: Add dynamic memory files to Products using the Sentinel LDK-EMS graphical user interface.
SM-12832	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. **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.
SM-19045	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. **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.
SM-52262	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.
SM-68428	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. **Workaround:** Specify the locale for the customer.

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

Ref	Issue
	The Sentinel Remote Update System (RUS utility) is not supported for Mac systems. **Workaround**: To obtain a fingerprint, use Sentinel Admin Control Center.

Ref	Issue
SM-116811	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: > When upgrading RTE version 8.13 or earlier to RTE version 8.15 or later *OR* > When downgrading RTE version 8.15 or later to RTE version 8.13 or earlier **Workaround**: After installing the desired version of the RTE, do either of the following: > Install the desired version of the RTE a second time. After performing the second installation, the **hasplmd** daemon starts automatically. *OR* > Start the **hasplmd** daemon manually by entering the command: **systemctl start hasplmd**
SM-94994	Given the following circumstances: > An RTE without legacy drivers is installed on a new machine. > An RTE with legacy drivers is installed afterward on the machine. 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. **Workaround:** Using Admin Control Center, generate a diagnostic report, and contact Thales Technical Support.
SM-82475	Given the following situation: > 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**. 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.

Ref	Issue
SM-76660	Given the following circumstances: 1. Windows is installed on a Mac machine with Boot Camp. 2. An SL license is installed in the Windows system. The Secure Storage ID may change and cause Feature ID 0 to be flagged as "cloned". **Workaround**: Do not install the SL license in the Windows system. Have your application consume a network seat from a cloud license.
SM-70131	The Sentinel LDK License Manager (process hasplms.exe) hangs intermittently and reaches a very high CPU utilization (approximately 1.9 GB). **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.
SM-59868	An application linked with **libhasp_windows_bcc_vendorld.lib** requires Sentinel LDK Run-time Environment on the machine.
SM-546	Given the following circumstances: > 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) The protected application may fail. **Workaround:** Include the External License Manager (hasp_rt.exe) with the protected application.
LDK-14971	Given the following circumstances at a customer site: > 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. A rehost operation may fail with the message HASP_REHOST_ALREADY_APPLIED. **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.

Ref	Issue
LDK-12547	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. **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.)
LDK-10670	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. This issue has been reported to Razer.
LDK-9044	Given the following circumstances: 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. 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.) **Workaround:** Switch the USB controller to USB 2.0 mode.
LDK-8480	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.) **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().

Sentinel LDK Envelope and Data Encryption for Windows Platforms

General

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

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	Given the following circumstances: 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. 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. **Workaround:** Do not use the current version of the IObit product, *OR* do not use SL AdminMode licenses until this issue is resolved. (You can use SL UserMode licenses.)
SM-65381	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. **Workaround:** Ensure that **hasp_rt.exe** is present in the protected folder.

SM-114641	When running an enveloped application that has the function **fork()**, the error "Segmentation fault (core dumped)" occurs.
	Workaround: The following workarounds are available for executables and shared libraries (use one of these):
	> Disable Intel Control Flow in compilation using:
	 -fcf-protection=none
	> Compile the application with **-no-pie** (for executables only)
	> From a terminal, execute the application using:
	 LD_BIND_NOW=1 <protected application>
	> Use a function pointer in code instead of directly calling 'fork':
	<pre>pid_t (*fun_ptr)() = ⋔
	    id = fun_ptr();</pre>

Java

Ref	Issue
LDK-11195	When protecting a Java application, Envelope fails with the message "Serious Internal Error (12)". **Workaround:** If this error occurs, protect the Java application using either of the following techniques: > 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.
LDK-11418	For a Java 7 or 8 application that is protected with Envelope, the end user must use the following command line syntax to launch the protected application: > Java 7: Specify `java -UseSplitVerifier -jar `*`ProtectedJar`*`.jar` > Java 8 and later: Specify `java -noverify -jar `*`ProtectedJar`*`.jar` If the appropriate flag is not specified, the application may throw **java.verifyerror** when launched.
SM-10890	Given the following circumstances: > 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. The **Allows grace period after failed license check** check box should be modifiable. However, the check box cannot be changed. **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. **Note:** This grace period is not supported for Web applications.
SM-10969	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.

Ref	Issue
SM-98384	A protected WAR does not run successfully on WildFly Server 23.
SM-110174	Java class level protection and Data File protection in Windows Envelope for 64-bit applications are not supported under Wine.

.NET

Ref	Issue
SM-554	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.

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.

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.

Workaround:

Do the following:

1. Use .NET Framework 4.5.

2. Use

   CultureInfo.DefaultThreadCurrentCulture = new CultureInfo(...)

   instead of

   Thread.CurrentThread.CurrentCulture = new CultureInfo(...).

Ref	Issue

SM-25875	Given the following circumstances:
	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:
	`IntPtr hMod = Marshal.GetHINSTANCE (Assembly.GetExecutingAssembly().GetModules()[0])`
	The handle returned may not be correct, and as a result, an error will be generated.
	Workaround: You can call the GetModuleHandle system API of the Kernel32.dll to get the module handle.
	For example:
	`[DllImport("kernel32.dll", CallingConvention = CallingConvention.StdCall, CharSet = CharSet.Auto)] private static extern IntPtr GetModuleHandle(IntPtr lpModuleName); IntPtr hMod = GetModuleHandle(Process.GetCurrentProcess ().MainModule.ModuleName);`

SM-26578	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. **Workaround:** Call "Environment.Exit(1)" to exit the process.

Sentinel LDK Envelope and Data Encryption for Linux

Ref	Issue
SM-28403	Given the following circumstances: > A Linux application is protected with Envelope, with protection against debugging. > The application calls the wait(&status) system call. This is equivalent to: `waitpid(-1, &status, 0)` The application may hang. **Workaround 1:** Call waitpid for a specific child process pid (pid > 0). **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.

Ref	Issue
SM-69080	A protected application may not handle signals properly when: > Background check is enabled, and > Signal handlers are registered by a thread created by the application. **Workaround:** Do one of the following: > Disable both background check and anti-debugging. (You can do this by specifying the following line command flags: `-b:0 --debug --memdump`) > (Preferred workaround) Register the signal handler in a main thread instead of a thread function. Thread function is one of the following: • 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	> 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	Due to reliability enhancements in Sentinel LDK under macOS, there is some performance impact in protected applications under macOS 10.13. A technical note will be issued that describes this issue and the option to disable these enhancements in favor of higher performance.