Sentinel LDK 9.0 with Sentinel EMS

RELEASE NOTES

Revision History

Part number 007-001944-001, Revision A, 2304-1

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.

CONTENTS

Sentinel LDK 9.0 with Sentinel 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

> View the previous version in English of the Sentinel LDK release notes.
>
> Download a ZIP file in English with all Sentinel LDK release notes.

Release: **9.0** | April 2023

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 not required when you are working with Sentinel EMS hosted on Thales servers.

Important: The Master key should be stored in a secure location. It is especially valuable because it could be 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

> **NOTE** If you are upgrading from a version of Sentinel LDK that is earlier than 8.5, 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: **9.0**

In this section:

Enhancements to Sentinel LDK Envelope

Sentinel LDK Envelope now supports the following functionality:

- **Enhanced V3 Engine**

The Windows V3 engine has been significantly enhanced to provide more robust and stable protection of Windows applications. As a result, Thales now recommends the use of the V3 engine as the engine of choice when protection applications.

The behavior of Sentinel LDK Envelope 9.0 is as follows:

- When you start Sentinel LDK Envelope 9.0 for the first time, by default the Windows engine used for applications in new projects is V3.
- If you open a project that was created in Sentinel LDK Envelope 8.5 or earlier, the protection engine in the Envelope Settings dialog box changes for that project to the setting that was in force when that project was created.

Once you manually change the Windows engine in the Settings dialog box and click OK, the engine you selected is applied for all applications that you add to any project, regardless of when the project was created.

> **Support for AppOnChip in the V3 Protection Engine**

The enhanced V3 protection engine now supports the use of AppOnChip functionality to protect applications that are licensed using HL (Driverless configuration) keys.

> **Support for .NET 7**

Sentinel LDK Envelope now supports .NET 7 applications.

Enhancements to Sentinel Run-time Environment Installer API

Sentinel Run-time Environment Installer API has been enhanced as follows:

> The **haspds_Install** function has been enhanced to support forcing installation of the RTE with legacy drivers if required.

Enhancement to V-Clock

The V-Clock in an SL key can now be set to a specific date and time, or to the date and time from the system clock on the machine where the V2C file is generated. This may be required, under certain circumstances, to re-enable a Feature that was blocked due to time-tampering.

> **NOTE** Before applying a V2C file to reset the V-Clock using the system clock, the user should ensure that the system clock is set to the current date and time.

Introduction of Sentinel Remote Update System (RUS)

The Sentinel Remote Update System (referred to as *RUS*) is an executable utility that you can send to your end users to enable secure, remote updating of the license and memory data of Sentinel protection keys after they are deployed.

The RUS utility can be used by the end user to:

> Generate a fingerprint of their machine to send to the vendor.

- Collect information about licenses on their machine to send to the vendor.
- Apply updates to licenses and memory data on the end user's machine.
- Transfer (*rehost*) an SL key from one of their computers to another, without any intervention by the vendor.

For more information, see Sentinel LDK Software Protection and Licensing Guide.

Licenses that you issue can only be updated by an RUS utility executable that is associated with your Batch Code. **RUS Generator** is a tool that performs this association. The RUS Generator can also be used to brand the RUS utility interface with your company information and with any other text or instructions that you want to add. For more information, see Sentinel RUS Generator.

Executable files (EXE) that contain V2C data is no longer supported while producing protection key update entitlements.

Expiration Date Licenses Can Now Be Assigned a Start Date

When defining license terms for a Feature with an expiration date in Sentinel EMS, you can now optionally define a start date for the license.

For example: If you want to provide a customer with a 30-day license that expires on a specific date, you can deliver the license any time prior to the start date specified in the license. The customer will be able to use the license only from the specified start date.

If no start date is specified, the license is active as soon as it is received and installed by the customer.

The following limitations apply:

- Must be supported by Sentinel EMS. Check the Sentinel EMS Release Notes or contact your Thales representative.
- Requires Sentinel Run-time Environment 9.12 or later.
- Only applicable for SL AdminMode and SL UserMode keys.
- Currently, start date and expiration date are calculated based on UTC and may not use the date and time that the user expects. In an upcoming release, the client time zone will be considered during license generation to ensure that the expected date and time are used.

Identity Strings Can Now Be Hidden

Identity strings used by cloud licensing can now be hidden in Sentinel Admin Control Center and in the **hasplm.ini** file on licensed users' machines. This prevents licensed users from sharing their identity strings with other users.

When hidden, the identity string is replaced in the serveraddr string in Admin Control Center with “*”.

Automatic detach remains supported even if the identity string is not visible in Admin Control Center or the hasplm.ini file.

Licenses that were detached before the identity string was hidden continue to be available without providing the identity.

For more information, see Sentinel Admin API Reference.

Rate Limiting for Cloud Licensing

Sentinel Licensing API now supports rate limiting for cloud licensing. As a result, it is now possible to implement rate limiting for cloud license requests issued by protected applications on customers' machines. The use of rate limiting prevents overloading the license server and improves the user experience if licensed user interactions with the applications are generating an excessive number of requests to the license server.

For more information, see Sentinel Licensing API Reference.

Rate limiting can be implemented for:

- Cloud license servers hosted on the vendor's network
- Cloud license servers hosted by Thales. For availability of this feature, check the Sentinel EMS Release Notes or contact your Thales representative.

Directories for Licensing API Have Been Renamed

The sample and API directories for Sentinel Licensing API in the Sentinel LDK installation have been renamed as follows:

From:

- **\Samples\Runtime\**
- **\API\Runtime\**

To:

- **\Sample\Licensing\**
- **\API\Licensing\**

These directories have been renamed for Windows, Linux, and Mac installation of Sentinel LDK. This change aligns the name of these directories from the legacy name of the API (that is, **Runtime API**) to the current name (**Licensing API**).

Enhancement to Sentinel Admin API

Access to Sentinel Admin API can now be restricted so that it is only available for users from the local network. This can be enforced using firewall rules. Administrator-level requests would be allowed only on a specific port or network interface (or both).

Admin Control Center Now Uses Session-Based Authentication

Password protection in Sentinel Admin Control Center now uses session-based authentication instead of basic authentication. This enhancement provides the option to log in securely from any machine without the need to configure a trusted client.

> **NOTE** If you have configured Admin Control Center to require login credentials, a user name is now required. If you have not defined a user name, use **admin** (the default user name) to log in to Admin Control Center.

Improved Help System for Admin Control Center

The help system for Sentinel Admin Control Center has been significantly improved. This new help system is provided when the user is working with Run-time Environment 9.12 and later.

Until now, the help system was implemented using simple HTML pages with very little navigation assistance.

The new help system is displayed in an independent browser window and provides:

- Context-sensitive help content
- A navigation pane
- Search capabilities
- Improved formatting and readability

These improvements will better assist users in working with Admin Control Center.

Additional Changes to Sentinel LDK

The Sentinel LDK High Availability for Cloud Licensing Configuration Guide has been incorporated into the Sentinel LDK Installation Guide. This configuration guide was formerly a standalone document.

Installation and Upgrades

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

Release: **9.0**

In this section:

> "Installing Linux and Macs Packages" below

Installing Linux and Macs 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

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: **9.0**

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: **9.0**

In this section:

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

Sentinel LDK Run-Time Environment version 9.12 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.)
>
>   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 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.9.12 - 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.9.12 - 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 5 > .NET 6 > .NET 7 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 applications with platform-specific functionality such as Windows Forms and Windows Presentation Foundation (WPF) work only on Windows platforms.

System	Supported Versions
Windows	x86 and x64 versions of the following: > Windows Server 2016 > Windows Server 2019 > Windows Server IoT 2019 > Windows Server 2022 > Windows Server IoT 2022 > Windows 10 IoT Enterprise 2019 LTSC > Windows 10 IoT Enterprise 2021 LTSC > Windows 10 22H2 > Windows 11 22H2 > Windows 11 ARM 22H2 (only protected with Licensing API) **NOTE** Support on Windows ARM machines with the ARM64-based processor: > 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. **Note:** Windows Insider Preview builds are not supported. The latest service packs and security updates must be installed.
Mac	> macOS 11.7 Big Sur > macOS 12.6 Monterey > macOS 13.3 Ventura Support on Mac machines with the ARM64-based processor: > Sentinel LDK is supported via Rosetta 2. > Sentinel Licensing API version 8.41 and later is supported natively. **Note:** The Sentinel Remote Update System (RUS utility) is not supported for Mac systems. To obtain a fingerprint, use Sentinel Admin Control Center.

System	Supported Versions	
Linux	**Linux Intel (x86-64)**	> OpenSUSE Leap 15.4 > Red Hat EL 9.1 > Ubuntu Server 22.04 > Ubuntu Desktop 22.04 > Debian 11.6 > CentOS Stream 9 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 8.0
Android	**Android ARM (32-bit)**	Android 11.x, 12.x, 13.x
	Android ARM (64-bit)	Android 11.x, 12.x, 13.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 18 for Mac > VMware Workstation 16 > VMware ESXi 6.7, 7.0 > Hyper-V Server 2019 (SL only) > Xen Project 4.17 > KVM (RHEL 9.1, Ubuntu 22.04 server, Debian 11.6) > Microsoft Azure > VirtualBox 7.0 > Docker (Linux) containers, including under Kubernetes > LXC containers > Amazon EC2 > GCP Compute Engine > Alibaba Cloud Elastic Compute Service

Web Browsers for Sentinel Admin Control Center

The latest versions of the following Web browsers are supported:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

This section describes requirements for Sentinel LDK.

Operating Systems

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 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 22H2 > Windows 11 22H2 **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 12.6 Monterey > macOS 13.3 Ventura 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 Support for Rosetta 2 Emulation.Sentinel LDK Envelope for Mac 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.)
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 15.4 > Red Hat EL 9.1 > Ubuntu Server 22.04 > Ubuntu Desktop 22.04 > Debian 11.6 > CentOS Stream 9 The latest service packs and security updates must be installed.

System	Supported Versions
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 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 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
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	9.12 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	29.1

> **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	9.12

Supported Platforms for Code Samples

The code samples are supported on the same platforms as listed for "Sentinel LDK Vendor Tools " on page 19.

> **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 11.3
	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17
	C# - .NET	.NET 6, .NET 7
	Note: An application linked with **libhasp_windows_bcc_vendorId.lib** always requires Sentinel LDK RTE on the machine.	
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, .NET 7
Licensing API for Linux	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17
	C	GCC
	C++	GCC
	C# - .NET Core	.NET 6, .NET 7

API	Programming Language	Tested Compilers
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
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
	C# - .NET Standard	.NET 6, .NET 7
Admin API for Linux	C	GCC
	C# - .NET Standard	.NET 6, .NET 7
Admin API for macOS	C	Clang 12.0.0 or later Xcode 12.0 or later
	C# - .NET	.NET 6, .NET 7
Envelope .NET Runtime API	C#	Microsoft Visual Studio 2019, 2022
Java Envelope Configuration API	Java	Oracle JDK 1.8 Oracle JDK 17 OpenJDK 17

API	Programming Language	Tested Compilers
Licensing Rest API for Windows	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17
Licensing Rest API for Linux	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 17
Licensing Rest API for macOS	Java	Oracle JDK 1.8 Oracle JDK 17 Open JDK 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
8.5, 9.0	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:

https://docs.sentinel.thalesgroup.com/softwareandservices/ldk/default.htm

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 EMS – Installation Guide	Details the prerequisites and procedures for installing Sentinel LDK Vendor Tools, Launchers for Sentinel 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.

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 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 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)	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. 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**.

Document	Description
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.

Resolved Issues

Release: **9.0**

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

Reference	Resolved Issue	Components
SM-97018	.NET Envelope runtime now supports dynamic GUI behavior. Error output of a .NET Envelope protected application now only outputs the error in the GUI when a GUI is available. If no GUI is supported, messages are automatically recorded in a console/eventlog.	Envelope-.NET
SM-119258	Sentinel LDK-EMS Web Services did not support adding dynamic memory files to Products.	Sentinel LDK-EMS
SM-132023	Resolved an issue with a manually-changed Envelope project file with AppOnChip enabled. Loading this special Envelope project file and re-enabling AppOnChip would sometimes cause the Envelope GUI to fail.	Envelope-GUI-Win
SM-132368	The combination of Sentinel Maze and WinNG Envelope protection would sometimes lead to an "integrity error" at runtime.	Envelope-NG
SM-134020	Under certain circumstances, UDP packets may be lost. Broadcast search now repeats the UDP transmission multiple times to overcome the loss of UDP packets.	Run-time Environment/API
SM-134453	An issue with DFP encrypted AI model files that could cause an application crash has been resolved.	Envelope-DataHASP, Envelope-Linux
SM-136775	The License Manager was not able to keep track of more than 2,000 clients' LM identifiers. This could result in incomplete information when listing detached licenses in the server Admin Control Center pages. The limitation of 2,000 LM identifiers has been removed.	Sentinel License Manager

Reference	Resolved Issue	Components
SM-137163	An issue which could lead to an application freeze after Envelope protection has been resolved. This issue would occur due to a deadlock when calling memcpy() in a secondary thread while loading the engine via dlopen().	Envelope-Mac
SM-139455	An issue with "large address" awareness of the Envelope command line application has been resolved. This issue would occur under very specific circumstances if the address space is already largely packed.	Envelope-GUI-Win
SM-139869	Previously, when a proxy was configured in ACC, the LM would attempt to resolve DNS names, even if they were not resolvable in the local network. This resulted in connection failures. Now, when a proxy is defined in ACC, the LM no longer attempts to resolve DNS names. Instead, it allows the proxy to handle DNS resolution.	Sentinel License Manager
SM-139963	When a seat was detached from a license with no vendor name defined, the H2R file would contain invalid information in the vendor name field.	Sentinel License Manager
SM-140043	On the Windows platform, the FQDN cloning scheme now compares the domain name, even if the domain name is empty.	Sentinel License Manager
SM-140200	Sentinel Admin API was not able to retrieve client identity information when the client identity was defined with multiple key IDs and admin_get was called using a specific key ID in the scope.	Sentinel Admin API

SM-141007	If the session username contains the "&" character, the GetInfo function would report the value in the XML structure as specified, resulting in an invalid XML file. For example:
	`<session username="AB&C" />`
	Now, the character is reported back as an XML entity. For example:
	`<session username="ABamp;C" />`
		Sentinel Licensing API

SM-141419	Support of asynchronous I/O in the file copy function of Windows update KB5022913 has been added.	Envelope-DataHASP, Envelope-NG
SM-141837	Envelope support for Qt Plugin DLLs in Windows V3 has been added.	Envelope-V3

Known Issues and Workarounds

The known issues in Sentinel LDK 9.0 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

Ref	Issue
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

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_vendorId.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.

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.

Ref	Issue
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.
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(...)**.

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);`

Ref	Issue
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.
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.