THALES

Sentinel LDK 8.2

RELEASE NOTES

Revision History

Part number 007-000667-002, Revision C, 2104-1

Disclaimer and Copyrights

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.
Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.
This document can be used for informational, non-commercial, internal and personal use only provided that:
• The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
• This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.
Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.
The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.
The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.
Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.
Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

Sentinel LDK 8.2 - Release Notes

About This Document

This document contains information about the latest release of the Sentinel LDK product, including new features, changes to the product, documentation, and known issues and workarounds.

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

Product Overview

Sentinel LDK (*Sentinel License Development Kit*) provides software publishers with strong anti-piracy and intellectual property protection solutions, offering unmatched flexibility in assisting you to protect your revenue and increase sales. The Sentinel system prevents unauthorized use of software, protects software copyrights and intellectual property, and offers multiple licensing models.

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 Master key and the Sentinel Developer 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 used in conjunction with Sentinel LDK and is attached to the Sentinel 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.

Every Sentinel EMS Server computer must have a Sentinel Master key connected.

Important: Keep these keys safe and allow only trusted personnel to use them. 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.

What's New in Sentinel LDK 8.2?

This section describes the main new features and enhancements.

> **NOTE** The Sentinel LDK 8.2 release includes all features and enhancements from earlier releases. Details on patches that were released between Sentinel LDK 8.0 and Sentinel LDK 8.2 are also included in this document.
>
> If you are upgrading from a version of Sentinel LDK that is earlier than 8.0, 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.

Sentinel EMS Uses Microsoft SQL Server 2019

When installing or upgrading to Sentinel EMS 8.2 on a Windows 10 machine, the installation procedure now installs or upgrades to Microsoft SQL Server 2019. Users who maintain their own SQL Server installation can link that installation to Sentinel EMS during Sentinel EMS installation.

Vendors who are upgrading from earlier version of Sentinel EMS can continue to work with Microsoft SQL Server 2014 under Windows 7.

The following table describes possible installation and upgrade scenarios.

Current OS	Vendor-Managed SQL Server	Existing EMS	Installation Options
Windows 10	None	None	Install Sentinel EMS. SQL Server 2019 is installed
Windows 10	MSSQL2019	None	Install Sentinel EMS. Use **Advanced** option to connect to existing SQL Server.
Windows 10	MSSQL2019	Yes	Upgrade Sentinel EMS. EMS maintains connection to the existing SQL Server.
Windows 7	Not relevant	None	LDK EMS installer notifies the user that Windows 7 is not supported with this release. A download link for LDK 8.0 is provided.

Current OS	Vendor-Managed SQL Server	Existing EMS	Installation Options
Windows 7	MSSQL 2014	Yes	Upgrade Sentinel EMS. User is notified that Windows 7 support will be removed in an upcoming release because it is not supported by Microsoft for security updates.

Run-time Environment Installation Without Legacy Drivers

Until now, the Sentinel LDK Run-time Environment (RTE) was always installed with legacy drivers. Sometimes, in rare cases, this would cause some instability on the machine.

Starting with RTE version 8.21, when installing the RTE for the first time on a Windows machine, the RTE is installed by default without legacy drivers. As a result, the RTE installation is more stable and reliable. If necessary, you can still force installation of the legacy drivers.

For more information, see the description of legacy drivers in the Sentinel LDK Software Protection and Licensing Guide.

Enhancements to Sentinel LDK Envelope

The enhancements described in this section have been implemented in Sentinel LDK Envelope

Class-Level Protection for Java Applications in Envelope

Sentinel LDK Envelope now provides class-level protection for Java applications.

Class-level protection and licensing can be used exclusively or together with method-level protection. Background checks can be performed for whichever protection type (class-level, method-level, or both) you select for the application.

Class-level protection provides:

- an additional protection layer that blocks Java reverse-engineering tools (for example: decompilers).
- high performance (compared to method-level protection).

> **NOTE** The current release only supports Windows runtime.

New Windows V3 Engine

The new Windows V3 engine is now available in Sentinel LDK Envelope for protecting Windows applications. This engine resolves certain compatibility issue in Envelope.

You can select the Windows V3 engine in the Envelope Settings screen. Thales recommends that you only use this engine when recommended by Technical Support.

Sentinel LDK Supports Android 11

Sentinel LDK now supports Android 11 applications, with the following limitations for APK protection:

- When compiled with Android API level 28 or earlier, protected APKs (both Java and native) are supported.
- When compiled with Android API level 29 or later, protected APKs (Java only) are supported.

Sentinel LDK Supports LXC Containers

You can now use Sentinel LDK to protect and license applications that execute in LXC containers. The support provided is similar to that which is currently provided for Docker containers.

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

Licensing API supports Apple Silicon

The latest Licensing API is a universal binary that supports both x86_64 architecture and arm64 architecture. Using this API, you can create a version of your macOS application that runs on both Apple Silicon and Intel-based Mac machines. To use the latest Licensing API, you need Xcode version 12 or later.

Releasing an Identity-Based License From a Remote Machine

Using Sentinel Licensing API, you can now program a protected application to release an identity-based license when the license is requested by the same identity client from a different machine. As a result, a user who leaves an application open on one machine can take over the license from a different machine.

For more information, see the Sentinel Licensing API Reference.

Web Service for Reports

You can now search for and generate standard and custom reports using a web service. For details, see the Sentinel LDK–EMS Web Services Guide.

Documentation Updates

The Sentinel LDK Envelope help system has been updated as follows:

- The description of the parameter **Strong Name Key file** for .NET assemblies has been enhanced to explain what happens when mixed mode or Windows-only shell is selected.
- The documentation provides considerations that apply when symbol obfuscation is selected for .NET assemblies.

Enhancements Introduced in Patches

This section described enhancements that were introduced in patches to Sentinel LDK 8.0 and are also included in this release.

Automatic Detach for Licenses

(This enhancement was included in Sentinel LDK Patch 12/2020.)

Sentinel LDK Run-time Environment now supports a new method for detaching licenses, referred to as **Automatic Detach**.

When Automatic Detach is enabled, a protected application automatically detaches a network seat from an SL key (that supports concurrency) when the application requires a license. As a result, the application can continue to operate even if the connection to the SL key is interrupted. The application retains the license for a predefined number of hours.

This method is especially useful when working with cloud licenses.

For details, see the description of detaching licenses in the Admin Control Center help system.

Sentinel EMS User Interface Customization

(This enhancement was included in Sentinel LDK Patch 12/2020.)

You can now configure the look and feel of Sentinel EMS Vendor Portal and Customer Portal with your own logo, favicon and color scheme. This lets you expand your brand identity to improve user experience. Only a user with administrative rights can view and access the UI Branding section in the Administration Console. For details, see the Sentinel EMS User Guide.

Simplified SL Key Creation and Updates in Sentinel EMS for Vendor-hosted Cloud Licenses

(This enhancement was included in Sentinel LDK Patch 12/2020.)

You can now use Sentinel EMS to produce an entitlement and push it to your cloud license server in a single operation.

When you create an entitlement, you can click **Produce & Push** to produce the entitlement and push the SL key or license update to your cloud license server machine. This simplifies the process and removes several steps which otherwise need to be performed manually. For a Product Key, clicking **Produce & Push** results in a new SL key on the license server. For a Protection Key update for a single key, this updates the selected key on the license server. For details, see the Sentinel EMS User Guide.

Strong Password Policy for Logging in to Sentinel EMS

(This enhancement was included in Sentinel LDK Patch 12/2020.)

You can now require strong passwords for users that log in via Sentinel EMS Vendor Portal or a Web Service.

This applies both for new and existing users. Passwords must meet the following criteria:

- 8 to 30 characters long
- At least one uppercase letter (A-Z) and one lowercase letter (a-z)
- At least one number (0-9) or special character (! @ # $ % ^ & * ( ) _ - + = , .)

For new installations, this policy is applied by default.

When upgrading from an earlier version, the setting for this policy remains unchecked to maintain seamless access. You can apply the strong password policy if needed. For details, see the Sentinel EMS Configuration Guide.

Strong Password Policy for Logging in to the Admin License Manager

(This enhancement was included in Sentinel LDK Patch 12/2020.)

When setting or changing the password for accessing Sentinel Admin License Manager (using Admin Control Center or Sentinel Admin API), you must now specify a strong password. The password must satisfy the following requirements:

- At least eight characters long
- At least one uppercase letter (A-Z) and one lowercase letter (a-z)
- At least one number (0-9) or special character (for example: ! @ # $ % ^ & * " ( ) . , - +)

These requirements are enforced when a password is added or changed. There is no warning or action required if the existing password does not satisfy these requirements.

Defining Password for Sentinel EMS Users

(This enhancement was included in Sentinel LDK Patch 12/2020.)

Sentinel EMS users can now set their own password.

When you create a user, you can now either specify the user's password yourself or generate an email asking the user to set their password. For details, see the Sentinel EMS User Guide.

Custom Clone Protection Scheme Enhancement

(This enhancement was included in Sentinel LDK Patch 12/2020.)

For increased security, you can now require a license to meet all of the clone protection criteria that matched when the license was generated.

Each custom clone protection scheme contains the **Minimum Required Criteria** parameter that states how many of the selected identifiers must be met for the license to be validated. For stronger protection against cloning, you can select the option **All identifiers present at license generation must exist and match at runtime**. When selected, all of the identifiers that were selected and were present when the license was generated must exist and match when the license is validated to run the protected application.

For example, suppose the **Minimum Required Criteria** in your custom clone protection scheme requires 4 out of 5 criteria in the fingerprint. If this new option is selected, and all 5 of the criteria were present when the license was generated, then all 5 of the criteria must match the fingerprint at runtime, even though the custom clone protection scheme requires only 4.

For details, see the Sentinel EMS User Guide.

Detached Licenses Now Use the "Platform Default" Clone Protection Scheme

(This enhancement was included in Sentinel LDK Patch 12/2020.)

When a license is detached from an SL key on a license server, the detached license is now assigned the **Platform Default** clone protection scheme. This ensures that the detached license is protected with the most appropriate clone protection scheme for the platform where the license will be attached.

> **NOTE** The **Platform Default** scheme is assigned regardless of whether clone protection was enabled for the Product license on the license server from which the license was detached.

For details, see Sentinel EMS User Guide.

Enhancements to Sentinel LDK Envelope

(This enhancement was included in Sentinel LDK Patch 12/2020.)

Electron Support

Envelope for Windows has been enhanced to support Electron applications.

Extended Support for .NET

Applications protected using Sentinel LDK Envelope now support the .NET v5.0 framework.

Improvement to Envelope User Interface for .NET and Java Applications

When the **Feature ID** is set to Default (0), Envelope now sets the parameter **Frequency** to **Once per program** and disables the setting to define frequency for method-level protection. This blocks the user from accidentally defining an invalid request. (If checking the protection key is already defined to be performed once, then defining the frequency of checks is not applicable.)

Support for Oracle Java 11 and Open JDK 14

Sentinel LDK Envelope under Windows now supports the protection of Oracle JDK 11 and Open JDK 14 applications for Windows, Linux, and Mac. This includes applications that use the Java Platform Module System (JPMS).

As part of the protection process, Envelope generates files that contain the command required to execute module-based applications on different platforms. You must modify these files before using them to execute the protected application.

For details, see the help system for Sentinel LDK Envelope.

Updated External License Manager

(This enhancement was included in Sentinel LDK Patch 10/2020.)

External License Manager version 24.4 is included in this patch. This provides optimal compatibility with the customized Vendor Library version 8.15 that you can download using the Master Wizard.

Stronger Security for Admin License Manager Configuration

(This enhancement was included in Sentinel LDK Patch 12/2020.)

When you enable remote access to Admin Control Center, you must now enable password protection for accessing the configuration pages for Admin Control Center. You have the option of requiring a password to access *any* part of Admin Control Center

Cloud Licensing Supports Multiple Key IDs for Client Identities

(This enhancement was included in Sentinel LDK Patch 12/2020.)

When creating a client identity for cloud licensing and specifying the **Limit to Key ID** parameter in Admin Control Center (or Admin API), you can now specify multiple key IDs for a given client identity.

Domain Name Can Now Be Used to Restrict User Access to a License Server Machine

(This enhancement was included in Sentinel LDK Patch 12/2020.)

Admin Control Center enables a customer to specify which users can access a license on a license server machine.

You can now include domain names as part of the restrictions that they specify for this purpose. For example, you can now specify:

```
allow=username@hostname.domainname,...
allow=khsingh@noi-2n39623.thalesgroup.com
```

For details, see the description of the **User Restrictions** parameter on the **Configuration > Users** page of Admin Control Center.

Admin License Manager Can Now Listen on Port 80

(This enhancement was included in Sentinel LDK Patch 12/2020.)

Network licenses will be accessible even if port 1947 is not open in the firewall. To enable this enhancement, you must select the option **Listen for clients also on port 80** in the Admin Control Center configuration.

Reduced Installation Time for Run-time Environment

(This enhancement was included in Sentinel LDK Patch 12/2020.)

(Windows only) If the installed Run-time Environment is version 7.101 or later, it is no longer uninstalled before installing the new Run-time Environment. (This is because the driver binary has not been updated in the new version.) As a result, the installation time for the new Run-time Environment will be reduced if the same version of the driver binary is already installed in the system.

Enhanced Support for VMType3

(This enhancement was included in Sentinel LDK Patch 8/2020.)

Clone protection scheme **VMType3**, intended for cloud computing services, now supports Amazon EC2 in addition to Microsoft Azure. This provides enhanced clone protection for protected applications that execute on these platforms.

Sentinel License Generation API has been updated to support the enhancements for **VMType3**. The patch installs the updated version of Sentinel License Generation API on each machine where Sentinel Vendor Suite or Sentinel EMS is present.

For details, see the Sentinel LDK Software Protection and Licensing Guide.

Support for Cloud Licensing in Sentinel Admin API and ToolBox

(This enhancement was included in Sentinel LDK Patch 8/2020.)

Sentinel Admin API now contains functionality to support operations for cloud licensing. This enables you or your customers to automate actions required to implement and maintain cloud licenses.

The following operations are supported:

- Retrieve a single client identity
- Retrieve a list of client identities
- Create a client identity
- Update or disable a client identity
- Delete a client identity
- Unregister a machine

Sentinel LDK ToolBox has been enhanced to support these enhancements in Sentinel Admin API.

Enhancements to Sentinel LDK Envelope

(This enhancement was included in Sentinel LDK Patch 8/2020.)

Sentinel LDK Envelope provides support for the two official “long term support” versions of .NET Core framework (V2.1 and 3.1).

Envelope also supports protected applications to run on Linux x64, ARMHF and ARM64 platforms.

.NET Core applications with platform-specific functionality such as Windows Forms and Windows Presentation Foundation (WPF) work only on Windows platforms.

For details, see **.NET Core Version and Platform Support** in the Sentinel LDK Envelope help system.

What's Changed in Sentinel LDK 8.2?

This section describes significant changes to existing functionality or existing documentation in this Sentinel LDK release.

Rebranding of Gemalto to Thales

As part of the ongoing process to rebrand **Gemalto** to **Thales**:

- User interfaces and documentation for Sentinel EMS and Sentinel Vendor Tools have been rebranded for Thales.
- The directories under which Sentinel LDK and Sentinel LDK EMS are installed have been changed as follows:

From:

- *%ProgramFiles(x86)%\Gemalto Sentinel\Sentinel LDK*
- *%ProgramFiles(x86)%\Gemalto Sentinel\Sentinel EMS*

To:

- *%ProgramFiles(x86)%\Thales\Sentinel LDK*
- *%ProgramFiles(x86)%\Thales\Sentinel EMS*

For vendors who are upgrading from an earlier version, the existing */Gemalto Sentinel/* directories will be renamed to */Thales/* as above. In addition, for x86 machines, the following directory will be renamed:

From:

- *%ProgramFiles%\Gemalto Sentinel\Sentinel LDK*

To:

- *%ProgramFiles%\Thales\Sentinel LDK*

The path for launching Sentinel LDK Vendor Tools from the Start menu has been changed from **All Programs > Gemalto Sentinel > ...** to **All Programs > Thales > ...**

For example: **All Programs > Thales > Sentinel LDK > Vendor Suite**.

Support for Sentinel EMS Under Windows 7

Sentinel EMS can no longer be installed under Windows 7. You must install Sentinel EMS under Windows 10. However, vendors who are upgrading from Sentinel EMS 8.0 can continue to work under Windows 7 64-bit.

For more information, see "Sentinel EMS Uses Microsoft SQL Server 2019" on page 9.

Sentinel LDK Envelope for Mac - Help System

Sentinel LDK Envelope for Mac now provides context-sensitive help topics using an HTML5 help system.

Change to Sentinel LDK Envelope for Android

Sentinel LDK Envelope for Android now supports method protection for an APK that contains multiple DEX files.

Improved Run-time Environment Installer

Previously, completion of the upgrade of the Run-time Environment (hasplms.exe) was sometimes blocked if the existing Sentinel License Manager was locked by another process.

With the installer for RTE 8.21, if this situation occurs, the user can now select one of these options:

- Stop the process that is locking the Sentinel License Manager and then continue the Run-time Environment upgrade.
- Restart the machine. The Run-time Environment upgrade continues immediately after the restart.
- Cancel the upgrade.

Change to Documentation for Sentinel LDK Envelope

The following clarification has been added to the description of the **User Messages** function in the Projects pane of Sentinel LDK Envelope:

> **NOTE** Only modified and translated messages that were present at protection time are included in the protected application. Message that are provided or modified afterward do not affect previously-protected applications.

Sentinel LDK Envelope for NI RTEXE Is Discontinued

Sentinel LDK Envelope for NI RTEXE is no longer included in Sentinel LDK. You can continue to use this tool from Sentinel LDK 8.0.

Support for Sentinel LDK Envelope for NI RTEXE will be discontinued on 31-Dec-2021.

Data File Protection Plugin for Internet Explorer Is Discontinued

Data File Protection Plugin for Internet Explorer is no longer generated by the Master Wizard in Sentinel LDK 8.2.

You can continue to use this tool from Sentinel LDK 8.0.

Support for Data File Protection Plugin for Internet Explorer will be discontinued on 31-Dec-2021.

Changes to Sentinel EMS Configuration and Usage

Sentinel EMS User Interface Customization

You can now configure the look and feel of Sentinel EMS Vendor Portal and Customer Portal with your own logo, favicon and color scheme. This lets you expand your brand identity to improve user experience. Only a user with administrative rights can view and access the UI Branding section in the Administration Console. For details, see the Sentinel LDK–EMS Configuration Guide.

License File Name (V2C) Configuration File Name

You can now configure the order of the elements in a V2C file name (naming pattern). In earlier versions, you could only select the elements to include in a V2C file name. For details, see the Sentinel LDK–EMS Configuration Guide.

Simplified SL Key Creation and Updates in Sentinel EMS for Vendor-Hosted Cloud Licenses

You can now use Sentinel EMS to produce an entitlement and push it to your cloud license server in a single operation.

When you create an entitlement, you can click **Produce & Push** to produce the entitlement and push the SL key or license update to your cloud license server machine. This simplifies the process and removes several steps which otherwise need to be performed manually. For a Product Key, clicking **Produce & Push** results in a new SL key on the license server. For a Protection Key update for a single key, this updates the selected key on the license server.

For configuration details, set the cloud licensing options in the Administration Console, as described in the Sentinel LDK–EMS Configuration Guide.

For usage details, see the section on producing and pushing an entitlement in the Sentinel LDK–EMS User Guide.

Rehosting Behavior Changed for Entitlements with Conflicting Rehost Values

When an entitlement contains Products with different **Rehost** values, licenses are generated as follows:

- If the **Rehost** value for one or more Products is set to **Disable**, then rehosting is disabled for all Products in this entitlement.
- If the **Rehost** value is set to **Enable** for one or more products, and no Product is set to **Disable**, then rehosting is enabled for all Products in this entitlement.
- If the **Rehost** value for all Products is set to **Leave as it is**, then the rehosting value defined in the Protection Key is not affected and remains as is.

You can see the results in Sentinel Admin Control Center. For details on setting the **Rehost** value, see the Sentinel LDK–EMS User Guide.

Planned Changes in Upcoming Sentinel LDK Releases

The following changes are planned for upcoming Sentinel LDK releases. If you have any feedback or questions, feel free to contact Thales Support.

- Sentinel LDK 8.2 is the final release where Sentinel EMS is supported under Windows 7 64-bit. The use of Windows 7 is limited to vendors who are upgrading from LDK 8.0. Any new installations of EMS for LDK 8.2 is only be supported on Windows 10.

  Note that this applies to Sentinel EMS only. The Sentinel LDK 8.2 Vendor Suite will remain fully supported under Windows 7.

- Support for Business Studio and for Business Studio Server will be dropped in one of the next releases or service packs for Sentinel LDK .

Upgrading From 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 8.2 from Sentinel LDK v.7.3 through v.7.8, all non-English locales of Customer contacts and Channel Partner contacts in Sentinel EMS are converted to the English locale. If this issue is applicable to your installation of Sentinel EMS, make sure to read this technical note before upgrading to Sentinel LDK 8.2.

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

- The procedure for upgrading to Sentinel LDK 8.2 has been tested only for Sentinel LDK v.7.9 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 EMS, or both.)

Migrating from Sentinel HASP to Sentinel LDK 8.2 continues to be supported. For details, see the *Sentinel HASP to Sentinel LDK Migration Guide* provided with Sentinel LDK 8.2.

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

Security Updates

There are no known security issues in this release, and this release does not resolve any known security issues relating to Sentinel products.

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

Supported Platforms for Sentinel LDK – End Users

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.

Sentinel LDK Run-time Environment, Protected Applications

Sentinel LDK Run-Time Environment version 8.21 is provided for Windows, Mac, and Linux Intel 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 Run-time Environment to version 8.21 migrates existing SL AdminMode licenses a new secure storage. Once this occurs, you cannot downgrade the Run-time Environment to an earlier version. Downgrading the Run-time Environment 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.8.21 - version-restricted option:**

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

- **When using customized vendor API libraries v.8.21 - 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 Run-time Environment, and protected applications (with or without the Run-time Environment), 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 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 **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 7 SP1 > Windows 8.1 SP1 > Windows Server 2008 R2 SP1 > Windows Server 2012 R2 > Windows Server 2016 > Windows Server 2019 > Windows 10 IoT Enterprise 2019 LTSC > Windows 10 20H2 **Note:** Windows 10 Insider Preview builds are not supported. The latest service packs and security updates must be installed.
Mac	> macOS 10.14 Mojave > macOS 10.15 Catalina > macOS 11.0 Big Sur **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 15.2 > Red Hat EL 7.9, 8.3 > Ubuntu Server 18.04, 20.04 > Ubuntu Desktop 20.04 > Debian 10.7 > CentOS 8.3 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 Run-time Environment was tested on Linux platforms with Wine 6.0

System	Supported Versions	
Android	**Android ARM (32-bit and 64-bit)**	Android 9.x, 10.x, 11 **Note:** For Android 10.x and 11, APKs compiled with API level 29 and later only support Java protection. If you require native code protection for Android 10.x and later, contact Thales support.
	Android Architecture	The following architectures are supported: > armv7 > armv7a > arm64
	Android ABI	Sentinel LDK Envelope supports Android applications designed for the following Android application binary interfaces: > armeabi > armeabi-v7a > arm64-v8a
	Note: Data file protection is not supported for Android 7.x and later.	
Virtual Machines	The VM detection and VM fingerprinting capabilities provided by Sentinel LDK have been validated on the following technologies: > Parallels Desktop 16 for Mac > VMware Workstation 15 > VMware ESXi 6.5, 6.7 > Hyper-V Server 2019 (SL only) > Xen Project 4.14 > KVM (RHEL 8.3, Ubuntu 20.04 server, Debian 10.x) > Microsoft Azure > VirtualBox 6.1.x > Docker (Linux) containers > LXC containers	

Web Browsers for Sentinel Admin Control Center

> Microsoft Edge - latest version

> Mozilla Firefox - latest version

- Google Chrome - latest version
- Safari - latest version
- Microsoft Internet Explorer (32-bit) version 11

Supported Platforms for Sentinel LDK – Vendors

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.

Sentinel EMS Service

System	Supported Versions
Windows	x86 and x64 versions of the following: > Windows Server 2016 (only x64) > Windows Server 2019 > Windows 10 20H2 **Note:** Windows 10 Insider Preview builds are not supported. The latest service packs and security updates must be installed.

Sentinel EMS Database

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 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 EMS

Supported Browser	HTTPS	HTTP
Google Chrome version 80 or later	✓	✓
Mozilla Firefox version 84 or later	✓	✓
Microsoft Edge (Chromium-based)	✓	✓
Microsoft Internet Explorer version 11	✓[1]	✓

[1]Java applets are used for protection key-related operations.

> **NOTE** The Mac Safari Web browser is *not* supported for Sentinel EMS (both Vendor Portal and Customer Portal) in this release.

Sentinel LDK Vendor Tools

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

System	Supported Versions
Windows	x86 and x64 versions of the following: > Windows 7 SP1 > Windows 8.1 SP1 > Windows Server 2008 R2 SP1 > Windows Server 2012 R2 > Windows Server 2016 > Windows 10 20H2 **Note:** Windows 10 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 10.15 Catalina > macSO 11.0 Big Sur 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 15.2 > Red Hat EL 8.3 > Ubuntu Server 20.04 > Ubuntu Desktop 20.04 > Debian 10.7 > CentOS 8.3 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 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 Run-time Environment 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

NOTE A given version of the Vendor library is compatible with newer versions of the Run-time Environment . However, to support the enhancements in a given version of the Run-time Environment, 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

> **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 32.

> **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 2009, 2010, 2014
	C	Microsoft Visual Studio 2015, 2017, 2019 C++ Builder Developer Studio 2006
	Visual Basic .NET	Microsoft Visual Studio 2017, 2019
	C#	Microsoft Visual Studio 2017, 2019
	C++	Microsoft Visual Studio 2015, 2017, 2019 C++ Builder Developer Studio 2006 GCC
	Delphi	Delphi 10.4
	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
	C# - .NET Core	.NET Core 3.1
	C# - .NET	.NET 5
	Note: An application linked with **libhasp_windows_bcc_vendorId.lib** always requires Sentinel LDK Run-time Environment on the machine.	
Licensing API for macOS	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
	C	Clang 9.0.0 or later Xcode 9.0 or later

API	Programming Language	Tested Compilers
Licensing API for Linux	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
	C	GCC
	C++	GCC
	C# - .NET Core	.NET Core 3.1 .NET 5
Licensing API for Android	Java	Oracle Java Developer Kit 1.8
License Generation API for Windows	C, C#, Visual Basic .NET	Microsoft Visual Studio 2017, 2019
	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
License Generation API for Linux	C	GCC
Activation API for Windows	C	Microsoft Visual Studio 2015, 2017, 2019 You may need to convert the provided workspace for the VS version used.
	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
Activation API for macOS	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
Activation API for Linux	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14

API	Programming Language	Tested Compilers
Runtime Environment Installer	C	Microsoft Visual Studio 2015, 2017, 2019
	MSI	InstallShield 12 InstallShield 2013 or later
Admin API for Windows	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
	C, C#, C++, Visual Basic .NET	Microsoft Visual Studio 2017, 2019
Admin API for Linux	C	GCC
Admin API for macOS	C	Clang 9.0.0 or later Xcode 9.0 or later
Envelope .NET Runtime API	C#	Microsoft Visual Studio 2015, 2017, 2019
Java Envelope Configuration API	Java	Oracle Java Developer Kit 1.8 Oracle Java Developer Kit 11 Open JDK 14
Android Envelope	Java	Oracle Java Developer Kit 1.7, 1.8 Android Studio 3.6

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	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

Sentinel LDK Version	Firmware Version on...		
	Sentinel HL (Driverless Configuration) Keys	**Sentinel HL (HASP Configuration) Keys**	**(Legacy) Sentinel HASP Keys**
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 Run-time Environment is installed. View the list of keys in Admin Control Center.

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 8.2. Thales will continue to accept queries for issues related to these platforms and compilers, and will attempt to provide information to resolve related issues.

Platforms for Protected Applications for End Users

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

- Android 8.x
- macOS 10.13

Sentinel LDK Documentation

The documents and online help systems described below are provided in this release of Sentinel LDK.

> **NOTE** Most major Sentinel LDK documentation can be found online at:
> https://docs.sentinel.thalesgroup.com/ldk/home.htm

Documents

Sentinel LDK documents (PDF files) can be found:

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

Document	Description
Sentinel LDK Installation Guide	Details the prerequisites and procedures for installing Sentinel LDK Vendor Tools, Sentinel EMS Server, and the Run-time Environment.
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.

Document	Description
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 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 Quick Start Guides	Provides 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 EMS to satisfy the requirements of your organization.
Sentinel LDK-EMS User Guide	Provides the Sentinel 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 EMS user interface.)
Sentinel LDK-EMS Web Services Guide	Provides the developer with an interface for integrating Sentinel EMS functionality into the vendor's existing back-office systems.
Integrating Sentinel 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 EMS Server.
Migration Guide: Sentinel HASP to Sentinel LDK	Describes how to migrate from Sentinel HASP to Sentinel LDK and describes how to migrate your Business Studio Server database to a Sentinel EMS database. This guide also describes the Business Studio Server API for Sentinel EMS.

Document	Description
Additional Guides for Migrating to Sentinel LDK	These guides describe how to migrate to Sentinel LDK from: > Hardlock > SmartKey > Sentinel SuperPro > HASP HL > HASP4 > Sentinel Hardware Keys

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**

Help Systems - Sentinel LDK and Sentinel EMS User Interfaces

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

Online Help System	Description
Sentinel LDK 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.

Online Help System	Description
Sentinel EMS	Provides the Sentinel 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.

Help Systems – Sentinel LDK APIs

Documentation for the Sentinel LDK APIs described below can be found:

- On the Sentinel Customer Community web site, at: https://docs.sentinel.thalesgroup.com/ldk/home.htm
- where Sentinel LDK is installed, under: **%ProgramFiles(x86)%\Thales\Sentinel LDK\API**

Sentinel LDK API	Description
Activation API Reference	Provides function calls that can be used to simplify the process of SL key activation at the customer site. (Deprecated – replaced by Sentinel EMS Web Services.)
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.

Sentinel LDK API	Description
Run-time COM API	Provides the developer with access to Sentinel HASP Run-time Environment functionality, through an interface written for the Microsoft Component Object Model (COM).
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 EMS Web Services	Provides the developer with an interface for integrating Sentinel EMS functionality into the vendor's existing back-office systems. (Documentation is available from the **index.html** menu under **%ProgramFiles(x86)%\Thales\Sentinel EMS\EMSServer\webapps\ems\Docs**
License Generation API Reference	Provides access to the power and flexibility of Sentinel protection keys without the need to employ the full Sentinel EMS system. 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.

Software and Documentation Updates

Thales recommends that you frequently visit the Sentinel downloads page to ensure that you have the most recent versions of Sentinel LDK software and documentation, and for documentation in other languages.

Resolved Issues

This section describes issues that were reported by vendors and that have been resolved in this release of Sentinel LDK.

Reference	Resolved Issue	Components
SM-89441	Fixed description of <detachable> tag in Licensing AP reference.	Documentation
SM-90175	Added information in the Sentinel LDK–EMS Configuration Guide with best practices for users facing issues with sending email notifications from Sentinel EMS. In the Administration Console, Thales recommends using an identical value for User Name (in the Outgoing Server Settings area) and for all E-mail From settings on that page.	Documentation
SM-93334	Added information in the Sentinel LDK–EMS Configuration Guide about configuring Trusted IP Address as part of the process of enabling cloud licensing.	Documentation
SM-80129	Envelope would fail under certain circumstances for Unity.exe.	Envelope
SM-80748	Executables would have their PE checksum calculated incorrectly after protection.	Envelope
SM-81710	When using ApponChip protection, Envelope would fail when loading a QT application.	Envelope
SM-82184	With macOS 10.15 and its SDK, Apple introduced pointer padding for the symbol table. Previous SDK builds would cause an error "malformed binary" with padding. macOS 10.15 SDK causes the same error without padding.	Envelope
SM-88578	Projects build with Xcode 12 introduce a small change in the Mach-O file structure. Envelope did not handle these changes correctly.	Envelope
SM-90631	INTERNAL_IMP_GATES option would cause protection error 815.	Envelope
SM-91262	The trigger for alignment of the symbol table (LC_SYMTAB - symoff) has been corrected.	Envelope

Reference	Resolved Issue	Components
SM-93167	The feature protecting against memory dumps would sometimes impact the startup of the protected application.	Envelope
SM-93750	The ABSOLUTE bytes were not padding correctly for TLS relocation.	Envelope
SM-94005	(macOS) vm_protect failure when code section starts at page boundary.	Envelope
SM-95310	For an overlay application, the static integrity check was not disabled by default. As a result, a problem would result when the application would attempt to read overlay data from the end of file, including the integrity signature.	Envelope

Issues Resolved in Version 8.0.1

The following issues were resolved by the upgrade from Sentinel EMS 8.0 to Sentinel EMS 8.0.1

Reference	Resolved Issue	Components
SM-78725	Sentinel EMS would fail to generate HL and SL UserMode licenses when the configuration option Cloud Licensing was enabled. The following error message was displayed: *Could not generate the license because: XML schema validation failure occurred. no declaration found for element 'cloud_licensing'. The line number of the end of the text where the exception occurred is 15.*	LDK-EMS
SM-79148 SM-79207	The customized RTE for Linux generated by Sentinel EMS did not contain the 32-bit haspvlib.	LDK-EMS
SM-79150	After upgrading to Sentinel EMS 8.0: When creating a Product with read-only memory and with no text, Sentinel EMS would calculate string length the memory incorrectly. When text was written to the memory afterward, the following message was displayed: *The memory segment is too small to contain this text. Make the text shorter.*	LDK-EMS
SM-78970	Sentinel EMS 8.0 would not operate correctly when installed under a non-English version of Windows.	LDK-EMS

Resolved Issues in Patches

The following issues were resolved in Patches 8/2020, 10/2020, and 12/2020 for Sentinel LDK 8.0 and are also resolved in this release.

Reference	Resolved Issue	Components
SM-90271	Documentation for Sentinel License Generation API has been corrected as follows: > Placement of the <minimum_rte_api_version> tag has been moved from the Product level of the XML code to the protection key level. This parameter relates to all the Products in the protection key, not to a specific Product. > Documentation for the <rehost> tag has been updated to indicate that the <minimum_rte_api_version> tag (if used), must be placed before the <rehost> tag in the XML code.	Documentation
SM-90954	.NET Engine would fails when adding a sample with an excessively long class name.	Envelope
SM-90780	A .ctor issue with Envelope.Net was resolved.	Envelope
SM-88548	Envelope would crash when adding .NET App.	Envelope
SM-86349	Applications protected with Envelope were not logging errors properly.	Envelope
SM-83026	Sentinel LDK Envelope 8.0 would fail while adding or protecting a .NET Core file.	Envelope
SM-82167	Under certain circumstances, when CodeObfuscation is set to **True**, Envelope would fail when protecting an application.	Envelope
SM-81865	When a debugger is in use, an application protected with AppOnChip would display the message **Debugger detected**. When the user dismissed the message box, the application would exit. Now, under the same circumstances, the message box displays a warning. The message can be dismissed without terminating the application.	Envelope

Reference	Resolved Issue	Components
SM-80815	When using AppOnChip, Envelope would fail during startup on old Intel processor platforms (Atom/Core2).	Envelope
SM-80748	The PE checksums for executables were calculated incorrectly after protection with Envelope.	Envelope
SM-86459	An issue in the External License Manager has been resolved	External License Manager
SM-80548	Under certain circumstances, when using Sentinel LDK Toolbox to generate a license update to enable Remote Desktop, the License Generation would fail with error 5009 ("License definition is invalid").	License Generation API
SM-79715	For the **VMType4** clone protection scheme, Generating a **Clear Clone** license would use CPU_UID instead of CPU for the fingerprint.	License Generation API
SM-82498	Under certain circumstances, the License Generation DLL would crash when generating a clearClone V2C.	License Generation API
SM-82026 SM-82827	Resolve a compatibility problem for PMType3 SL UserMode license definition.	License Generation API
SM-86082	(Linux) The upper limit for the number of sockets was too low, resulting in a login error in certain circumstances.	Licensing API
SM-83787	(Linux) Login calls would fail on Linux ARM64 platform. Output was “Bus error”.	Licensing API
SM-83674	Failed to call integrated Admin API without the vendor code.	Licensing API
SM-82050	Android sample would fail on Android 11 emulator/real device.	Licensing API
SM-77887	(Linux) SSH session was not detected if the customer runs an application using sudo or su. Licensing API	Licensing API
SM-90482	Calling Web Service update protection key with action of ConvertV2CToExe would result in a memory leak.	Sentinel EMS
SM-89552	Descriptive text for warning 2044 has been provided.	Sentinel EMS
SM-83309	When Sentinel EMS 8.0.1 is installed with Java 8 Update 261, Sentinel EMS would start correctly, but the login page was blank.	Sentinel EMS

Reference	Resolved Issue	Components
SM-83050	Given the following circumstances: > In the Sentinel EMS Administration Console, Sentinel EMS is configured to generate V2C files using the customer name in the name of the V2C file. > The name of a customer in Sentinel EMS contains a comma (for example: **test, name**). > An entitlement is generated for the above customer. The resulting V2C file could not be downloaded.	Sentinel EMS
SM-82260	Given the following circumstances: 1. In Sentinel EMS, copy an entitlement that has already been produced. 2. Add Products to the copied entitlement. The **Exclude All** button for Features is not accessible. Features must be individually excluded from the Entitlement.	Sentinel EMS
SM-80400	On the Entitlements page in Sentinel EMS: When performing a search using **Customer Name** and then sorting the results by **Ref ID 2**, an internal error would occur.	Sentinel EMS
SM-78585	The status value of product key should not be changed if relevant entitlement is disabled.	Sentinel EMS
SM-73900	Login would fail with error code 500 while running the EMS web service demo.	Sentinel EMS

Known Issues and Workarounds

The known issues in Sentinel LDK 8.2 that are likely to have the most significant impact on users are listed below, according to component.

Additional, less-common issues can be found here.

Sentinel LDK Installation

Ref	Issue
EMSLDK-5860	Installation of Sentinel LDK on a virtual machine may hang before completion of the installation process. **Workaround:** Interrupt and then restart the installation. If the problem occurs again, interrupt the installation. Enable 3D acceleration and increase the video memory of the virtual machine. Rerun the installation.
EMSLDK-7448	Sentinel EMS fails to install correctly on a machine where JRE 8 and earlier versions of JRE coexists. If a machine contains an earlier version of JRE, and you manually install JRE 8, then: > When installing Sentinel EMS, the Installer generates the error "Kindly Start the Service -SQLServer(EMSDATABASE) and then click OK". > When you click OK, the installation fails with multiple errors. This occurs because while upgrading to JRE 8 , the Java installer does not replace earlier JRE files from the **System32** directory. **Workaround:** Uninstall the earlier versions of JRE from your machine, and restart the Sentinel EMS installation. **Note:** > When upgrading to JRE 8, the Java installer also recommends that you uninstall earlier the version of JRE from your machine due to security concerns. For details, see: https://bugs.openjdk.java.net/browse/JDK-8073939 > This issue does not occur when your machine contains earlier versions of JRE, and the Sentinel EMS installation installs bundled JRE 8 reference.

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 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 EMS. **Workaround:** A solution for this issue is provided in the technical note available here.

Sentinel EMS

Ref	Issue
SM-12832	When a user clicks the link provided in an email (that is sent by Sentinel 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 EMS machine.
SM-19045	Customers who were associated with a channel partner prior to Sentinel LDK 7.7 will not be visible in Sentinel 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 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 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 in this release. **Workaround**: To obtain a fingerprint, use Sentinel Admin Control Center.
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-85061	When a user accesses Admin Control Center in Microsoft Internet Explorer, the search option in the **Client Identities** tab (**Configuration > Client Identities**) is not working correctly. **Workaround:** Use a Chrome or Firefox browser to access Admin Control Center.
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.
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.

Ref	Issue
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-10843	The FLV player (flvplayer.swf) under %ProgramFiles(x86)%\Thales\Sentinel LDK\VendorTools\VendorSuite\samples\DataProtection\flv\local no longer plays local FLV files in Microsoft Internet Explorer with Adobe Flash Player version 23 and later. The player can be used: > to play local FLV files in IE with Adobe Flash Player version 22 and earlier. > to play network FLV files in IE with all versions of Adobe Flash player. > to play local FLV files in all versions of desktop Adobe Flash player software.
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.
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.
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.
SM-98384	A protected WAR does not run successfully on WildFly Server 23.

.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.

Android

Ref	Issue
SM-38233	Data File Protection is not currently supported for Android 7 and later devices.
SM-96242	Envelope does not support command line executables on an ADB shell. This is because the license is installed in the application sandbox and permissions are elevated in androidmanifest file.

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.
SM-85003	Envelope does not support protection of applications if CET (Intel Control Flow Enforcement) is enabled during compilation. In Ubuntu 19.10 and later, **-fcf-protection** is enabled by default. **Workaround:** Use the **-fcf-protection=none** compilation flag at the time of compilation.

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 in August 2019 that describes this issue and the option to disable these enhancements in favor of higher performance.

Sentinel LDK Envelope for Android

Ref	Issue
SM-57733	An Android application that is protected using both Envelope and Licensing API fails on an Android gaming console. Envelope embeds the RUS utility in the application. Using the Licensing API also adds the RUS utility. This results in two RUS utility calls in the protected application and duplicate symbol names. **Workaround:** Thales recommends that you not protect an Android application with both Envelope and Licensing API. If you want to use both tools to protect an application, do the following: 1. Protect the application using Licensing API. 2. Remove RUS from the APK file. 3. Protect the application with Envelope.

