

Sentinel LDK v.7.10

RELEASE NOTES



Revision History

Part number 007-013811-004, Rev B

Copyrights and Trademarks

Copyright © 2020 Thales Group. All rights reserved.

Disclaimer

We have attempted to make this document complete, accurate, and useful, but we cannot guarantee it to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product. Gemalto is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions contained herein. The specifications contained in this document are subject to change without notice.

August 2019 Revision 2004-2

CONTENTS

Sentinel LDK v.7.10 - Release Notes	5
About This Document	5
Product Overview	5
Sentinel Vendor Keys	5
Obtaining Support	6
What's New in Sentinel LDK v.7.10?	7
Sentinel EMS Now Simplifies Online Application of License Updates	7
Additional Enhancements to Sentinel EMS	7
Optionally Enforce the Use of a Minimum Version of the Run-time Environment	8
Enhanced Support for Protected Applications in Docker Containers Under Linux	10
Added Support for .NET Core Assemblies	10
Improved Protection Against Computer Restoration Software	10
New Customizable End-User Messages in Sentinel LDK Envelope	10
Enhancements to Sentinel LDK Envelope for Linux	10
Enhancements to drcrypt Utility	11
License Generation API for Linux Is Now Included in Sentinel LDK Installation Drive	11
What's Changed in Sentinel LDK v.7.10?	11
Legacy Activation API Has Been Restored	11
Envelope and Master Wizard for Linux Are Now 64-bit Applications	12
Sentinel LDK Now Supports Only 64-bit Mac Platforms	12
The Location Where the System Searches for the Run-time API libraries for Java and .NET Has Changed	12
Legacy Engine in Sentinel LDK Envelope for Mac Has Been Discontinued	12
V-Clock Time for SL Keys Now Returned in C2V Files	12
Protecting Java Applications That Use Reflection APIs	12
Changes Introduced in Vendor Suite Patch KB0020220	13
Support for Protection of Android Libraries	13
Support for Custom Actions for a Failed Background Check in .NET Applications	13
Enhanced Protection for Python Applications Using Cython	13
Issues Resolved By This Patch	14
Planned Changes in Upcoming Sentinel LDK Releases	14
Documentation Corrections	14
Sentinel LDK Envelope for Mac - Help System	14
Upgrading From an Earlier Version of Sentinel LDK	16
Security Updates	16
Reporting a Security Vulnerability	16
Supported Platforms for Sentinel LDK – End Users	17
Sentinel LDK Run-time Environment, Protected Applications	17
Data File Protection Plugin for Internet Explorer	19
Web Browsers for Sentinel Admin Control Center	19
Supported Platforms for Sentinel LDK – Vendors	20

Sentinel EMS Service	20
Sentinel EMS Database	20
Web Browsers for Sentinel EMS	21
Sentinel LDK Vendor Tools	21
Supported Platforms for Code Samples	23
Tested Compilers for Code Samples	23
Current Firmware Version	25
Dropped Support	25
Platforms for Software Vendors and End Users	25
Dropped Support for 32-bit Linux Vendor Tools	26
Dropped Support for 32-bit Applications for Mac	26
Sentinel LDK Documentation	26
Documents	26
Getting Started Guides	28
Help Systems - Sentinel LDK and Sentinel EMS User Interfaces	28
Help Systems – Sentinel LDK APIs	29
Software and Documentation Updates	30
Resolved Issues	30
Known Issues and Workarounds	32
Sentinel LDK Installation	32
Sentinel EMS	34
End Users, Sentinel LDK Run-time Environment, License Manager, and Customer Tools	35
Sentinel LDK Envelope and Data Encryption for Windows Platforms	37
Sentinel LDK Envelope and Data Encryption for Linux	40
Sentinel LDK Envelope, Data Encryption, and Licensing API for macOS	40
Sentinel LDK Envelope for Android	41

Sentinel LDK v.7.10 - 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 have been changed since the initial release of Sentinel LDK 7.10 as follows:

- > The following topic has been modified with regard to upgrading from version 7.7: "[Upgrading From an Earlier Version of Sentinel LDK](#)" on page 16
- > The following topic has been added: "[Changes Introduced in Vendor Suite Patch KB0020220](#)" on page 13
- > Known issue "[SM-65381](#)" on page 37 has been added.

These release notes are subject to change. If you are reading the release notes that were installed with the product, Gemalto 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://sentinelldk.gemalto.com/Default.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.

Obtaining Support

You can contact us using any of the following options:

Business Contacts - To find the nearest office or distributor, use the following URL:

<https://sentinel.gemalto.com/contact-us-sm/>

Technical Support

To obtain assistance in using Gemalto products, feel free to contact our Technical Support team:

- > **Customer Support Portal** (preferred):
<https://supportportal.gemalto.com/csm?id=sentinel>
- > **Support Essentials** (Contact details, support plans, and policies):
https://supportportal.gemalto.com/csm?id=support_essentials
- > **For Issues Related to Using the Portal:** customerportalsupport@gemalto.com
- > **Phone:**
 - AMER: 800-545-6608 (US toll free)
 - International: +1-410-931-7520
 - EMEA/APAC: <https://supportportal.gemalto.com/csm?id=sentinel>
→ Click **Contact Us**
- > **E-mail** (Use if you cannot submit the technical issue via the portal):
technical.support@gemalto.com

Downloads

You can download installers and other updated components here:

<https://sentinelcustomer.gemalto.com/sentineldownloads/>

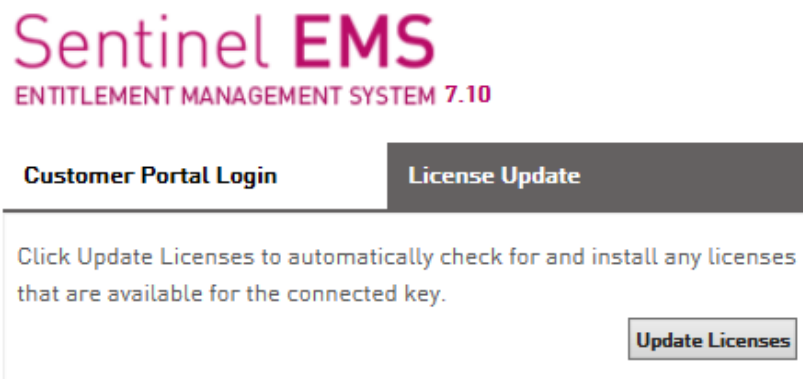
What's New in Sentinel LDK v.7.10?

This section describes the main new features and enhancements.

NOTE If you are upgrading from a version of Sentinel LDK that is earlier than v.7.9, 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 Now Simplifies Online Application of License Updates

End users can now apply multiple updates to one or more protection keys on their machines by simply visiting the Sentinel EMS Customer Portal and clicking the **Update Licenses** button. No login is required. When a user clicks the **Update Licenses** button, Sentinel EMS checks each protection key on the user's local machine and applies all outstanding license updates that have been issued for that key by the vendor.



Using this method, it is not necessary for end users to apply V2C files on their machines. When you issue a license update, you can simply instruct the end user to access the Customer Portal.

NOTE

- > Run-time Environment version 7.100 or later must be installed on the end user's machine.
- > The License Update tab cannot be used to apply license updates to SL Legacy keys.

Additional Enhancements to Sentinel EMS

Additional Improvement to Customer Portal

You can now add the Sentinel EMS Customer Portal directly to your site in an iFrame. This lets you keep your customers on your site. For details, see the *Sentinel LDK-EMS Configuration Guide*.

Improved Search Functionality in Sentinel EMS Screens

Previously, when you searched for a string in any Sentinel EMS screen, if your search string included multiple terms, Sentinel EMS used the OR operator to return all records that contain any of the specified terms. As a result, many irrelevant records were returned. For example, the search string "University of Melbourne" returned records such as "Ministry of Melbourne" and "University of Trent".

Now, Sentinel EMS uses the AND operator for these searches. As a result, only records that contain all significant search terms are returned.

In addition, you can now search for multiple instances of the same term to return all related entries, regardless of the number of times the term appears. For example, the search string "jo jo" will now return "Joseph Smith", "Joelle Joy Johnson", and "Cup of Joe"

Custom Reports

You can now limit the visibility of custom reports to users that have permissions for specific Batch Codes. For details, see the section on custom reports in the *Sentinel LDK-EMS User Guide*.

Recycled Sentinel HL Keys Can Now Be Re-used for Other Customers

Using the **Recycle Keys** feature in Sentinel EMS now makes it safe to re-use a recycled Sentinel HL key with any customer. Recycling an HL key removes all links between the specified key and customers. In addition, recycling an HL key completely removes the license data from the key and any uncompleted order data from Sentinel EMS.

New Web Services for Channel Partners

Several new Sentinel EMS web services were added to support channel partners. Functions such as creating, retrieving, searching for, updating, and deleting a channel partner are now available. For more details, see the *Sentinel LDK - EMS Web Services Guide*.

Optionally Enforce the Use of a Minimum Version of the Run-time Environment

This enhancement was included in the Sentinel LDK v.7.9 update.

API libraries that are customized for your vendor code are used by Sentinel LDK Envelope and Sentinel Licensing API to protect your applications. These libraries are generated by Gemalto specifically for your Batch Code. You download these customized vendor libraries using the Master Wizard when you introduce your Vendor keys.

The Master Wizard now offers you a choice of two types of libraries, each incorporating one of the options described below. The option that you select determines how protected applications interact with the Run-time Environment (the RTE). The available options are:

> **Version-restricted option** (Recommended for best security and reliability in the protected application)

For protected applications that require the RTE: With the version-restricted option, the applications will require a *minimum version* of the RTE (the earliest version that contains the latest important security and reliability enhancements). Use of the version-restricted option ensures that end users cannot downgrade to

an earlier version of the RTE and that they use a version of the RTE that provides the best quality together with all the latest security and reliability fixes. This restriction applies both for local deployment of the RTE and for deployment of the RTE on a remote license server machine.

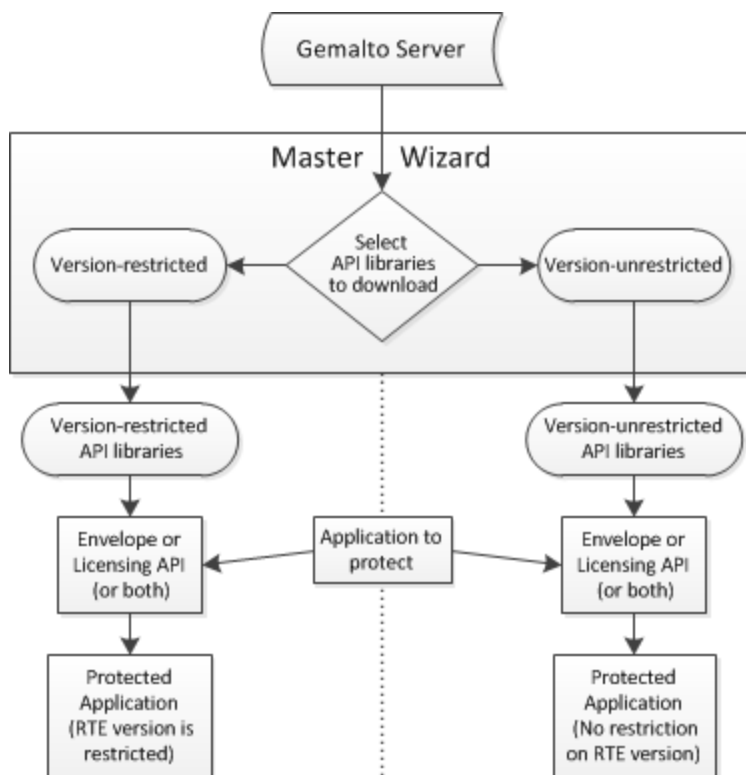
For each new release of Sentinel LDK, the required *minimum version* number is updated only if the RTE for that release contains significant security and reliability enhancements.

For example: The required *minimum version* of the RTE for applications protected with version 7.9 or 7.10 customized vendor libraries remains as RTE version **7.90**, because this version of the RTE contains the latest significant security and reliability enhancements. Later versions of the RTE contain less important enhancements and fixes.

> **Version-unrestricted option** (For compatibility with all versions of the RTE)

For protected applications that require the Run-time Environment: The applications will not check the version number of the RTE. Applications protected with this option can be used with all versions of the RTE. Select this option only if you want to avoid upgrading the RTE at end user sites. This option simplifies deployment, especially when network license servers are used, but does not guarantee that security and reliability fixes in later RTE versions are employed.

The following diagram illustrates this process:



NOTE With either option, users will need to upgrade their RTE if the protected application uses specific functionalities that require a later version of the RTE.

For details, see “Required Version of the Run-time Environment” in the *Sentinel LDK Software Protection and Licensing Guide*.

Enhanced Support for Protected Applications in Docker Containers Under Linux

You can now install Sentinel LDK Run-time Environment and certain SL keys within a Docker container under Linux. A new clone protection scheme (*VMType4*) is now available to protect applications that execute in a Docker container.

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

Added Support for .NET Core Assemblies

Sentinel LDK now supports the protection of .NET Core assemblies for versions 2.1 and 2.2 on Windows platforms using Sentinel LDK Envelope.

.NET Core contains only platform-independent features. Therefore, all platform-specific functionalities (such as GUIs) are not available, and certain limitations apply.

For example, Envelope-generated message boxes of all kinds will not work (because they are based either on System.Windows.Forms.MessageBox or on custom forms of System.Windows.Forms. In addition, .NET Core is mostly applicable for server-side applications, which may not have any GUI at all. All output messages will be logged only in the console due to the lack of message box support.

For details, see the Sentinel LDK Envelope help system.

Improved Protection Against Computer Restoration Software

The use of computer restoration software provides the ability to misuse certain types of protected applications. When computer restoration software is detected on a machine, a protected application that is not allowed to run on a virtual machine now returns the error code HASP_VS_DETECTED when either of the following is true:

- > The license type is Expiration Date, Executions, or Time Period.
- > The license allows detaching or rehosting operations.

New Customizable End-User Messages in Sentinel LDK Envelope

Messages related to the following protection settings in Sentinel LDK Envelope are now included in the customizable messages file:

- > Allow grace periods after failed license check
- > Run-time wait

Message IDs 5001 through 5007 were added and can be customized. Envelope supports the use of non-ASCII characters for customized messages.

(In the current release, these messages can only be customized for native Windows applications. For Java or .NET applications, these messages cannot be customized.)

Enhancements to Sentinel LDK Envelope for Linux

Sentinel LDK Envelope for Linux has been enhanced as follows:

- > New configuration and line command parameters enable you to disable the encryption of specific ELF binary sections in the protected application. This is useful if certain sections impact the runtime performance (in terms of memory consumption) on devices where swap area is not supported.
- > Sentinel LDK Envelope for Linux now supports certain uClibc modules by specifying the Envelope runtime pathname for an external module. This support can be provided on demand. Contact Technical Support for the list of supported external modules and for package delivery.

Enhancements to **dfcrypt** Utility

The **dfcrypt** line-command utility for encrypting and protecting data files has been enhanced as follows:

- > **dfcrypt** is now supported on Linux Intel platforms to protect data files using the **Version 2** data file protection mode. The protected files can be accessed (but not updated) by Linux applications under Linux Intel or Linux ARM.
- > When you protect a data using the **Version 2** data file protection mode in **dfcrypt** under Windows or Linux, you can now specify the encryption key to be used (up to 16 characters). If you do not specify the encryption key, a random key is generated. The protected application does not require the encryption key to access the protected data files.

License Generation API for Linux Is Now Included in Sentinel LDK Installation Drive

The Sentinel License Generation API for Linux is now available in the Sentinel LDK Installation Drive, including C samples (32-bit and 64-bit). See *\Linux\API\Licgen*.

What's Changed in Sentinel LDK v.7.10?

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

Legacy Activation API Has Been Restored

The following components of the legacy Activation API were removed from Sentinel LDK version 7.9, and restored in version 7.10:

- > \Windows\Installed\Legacy\API\Activation
- > \Windows\Installed\Legacy\Samples
- > \MacOS\Legacy
- > \Linux\Legacy

The legacy Activation API is no longer being maintained. Some new operating systems (for example, Ubuntu 18.04) no longer support the legacy Activation API. Gemalto recommends that you modify your applications to use Sentinel EMS Web Services.

Envelope and Master Wizard for Linux Are Now 64-bit Applications

For Linux Intel, Sentinel LDK Envelope and Master Wizard are now 64-bit applications. Envelope for Linux continues to support both 32-bit and 64-bit executables and shared libraries.

Sentinel LDK Now Supports Only 64-bit Mac Platforms

Sentinel LDK now supports macOS only on 64-bit machines. This applies to:

- > Vendor Tools (Envelope, Data Protection utility, Master Wizard)
- > Run-time Environment
- > Protected applications (executables and shared libraries)

If you use SL keys, be sure to use the Master Wizard to download the latest vendor libraries.

The Location Where the System Searches for the Run-time API libraries for Java and .NET Has Changed

In versions of Sentinel LDK earlier than 7.10, your customized Run-time API libraries for Java could be placed in any directory that was contained in the PATH environment variable. Due to security considerations, the PATH variable is no longer checked when the system searched for these libraries.

For more information on where to place these libraries, see the **readme.html** file under `\Samples\Runtime\Java` in the Windows, Linux, or MacOS folders on the Sentinel LDK Installation Drive.

Legacy Engine in Sentinel LDK Envelope for Mac Has Been Discontinued

Support for the legacy engine has been removed from Sentinel LDK Envelope for Mac. If you require the Legacy engine to protect your application, contact Technical Support.

V-Clock Time for SL Keys Now Returned in C2V Files

The V-Clock time for SL keys is now included in C2V files generated on an end user's machine when the application is licensed using Sentinel LDK v.7.10 or later. For SL AdminMode keys and SL Legacy keys, Run-time Environment v.7.100 or later must also be present on the machine.

Protecting Java Applications That Use Reflection APIs

A method for protecting Java applications that use reflection APIs (such as applications using the Spring Framework) has been included in the help documentation for Sentinel LDK Envelope (Windows and Linux).

Changes Introduced in Vendor Suite Patch KB0020220

Vendor Suite Patch KB0020220 is optionally installed as part of the Sentinel LDK 7.10 installation procedure. This patch introduced the following enhancements:

Support for Protection of Android Libraries

Sentinel LDK Envelope now enables you to protect Android library (AAR) files. Method-level protection is provided.

Certain restrictions apply. For more information, see the description of Android considerations in the Sentinel LDK Envelope help system.

Support for Custom Actions for a Failed Background Check in .NET Applications

Under certain circumstances, you may want to perform custom actions if a background check for the required product license returns a failed status. For example: For server applications, there may not be a user to see and respond to an error message regarding a failed background check.

The .NET Envelope Runtime API now enables you to provide alternative methods to notify users regarding a failed background check. For example, you can write a handler to generate an entry to a log or send an email alert.

For GUI-based applications, custom background checking is also useful. For example, your handler can display a custom alert, save all unsaved data and exit from the application.

For more information, see *Samples\Envelope\EnvelopeRuntime.NET\NET_Envelope_Runtime_API.html* in the Sentinel LDK installation.

Enhanced Protection for Python Applications Using Cython

Sentinel LDK Envelope now provides enhanced protection for Python applications by using Cython in the protection process. This works by first translating your sensitive Python modules into native modules (PYD/SO files), which are then protected using Sentinel Envelope.

This method provides a higher level of security because the additional compilation step lowers the code's abstraction level and enables Sentinel LDK Envelope to protect the application as code and not just as data. This results in more sophisticated protection measures.

This method of protecting your Python applications is available under Windows and Linux. For more information, see the Sentinel LDK Envelope help system for Windows or the *Sentinel LDK Envelope for Linux User Guide*.

NOTE When using Sentinel LDK Envelope with Cython to protect Python applications, certain unusual configurations of Python may generate errors. For example:

- > Python2 and Python3 installed on one machine
- > Python 32-bit and 64-bit versions installed on one machine
- > Using an old version of Python 2.7 (for example, 2.7.13 instead of the latest 2.7.16)

Issues Resolved By This Patch

Issue	Description
SM-65854	<p>Given the following situation:</p> <ol style="list-style-type: none"> 1. The vendor is using a high vendor code to generate licenses. 2. An SL AdminMode license has been generated with Sentinel LDK License Generation API v.7.10. 3. The license V2C file is applied successfully to the protection key on an end user's machine. 4. The License Manager on the user's machine is restarted. <p>The SL AdminMode license would disappear from the user's machine.</p>

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 Gemalto Support.

- > The 32-bit version of Sentinel LDK EMS will be moved to End-of-Development status. Future enhancements and support for new platforms will be provided for the 64-bit version, which will remain in General Availability status.
- > Sentinel LDK EMS will use OpenJDK instead of Oracle JDK. This is due to licensing changes by Oracle.
- > New Sentinel LDK Run-time Environment (RTE) installers will support installation without device drivers by default. This is to improve the reliability and experience of end users. An option to install the RTE with drivers will remain available for backward compatibility.
- > Support for 32-bit Linux on x86 will be dropped. 32-bit Linux on ARM will remain in General Availability status.

Documentation Corrections

This section describes last-minute changes to documentation for LDK 7.10.

Sentinel LDK Envelope for Mac - Help System

This section describes a correction to the help topic "Signing a Protected Application."

Replace step 4 in the procedure "How to manually sign an application after you protect it with Envelope" with the following:

Step 4

Before you submit your protected application to the Apple Notary service, you must sign the application using the **codesign** tool provided with the Apple Developer Tools (Xcode).

To sign your application, the **codesign** tool requires a number of hardened runtime entitlements.

1. Create a text file that contains the following entitlements:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>com.apple.security.device.usb</key>
    <true/>
    <key>com.apple.security.network.client</key>
    <true/>
    <key>com.apple.security.network.server</key>
    <true/>
    <key>com.apple.security.cs.allow-unsigned-executable-memory</key>
    <true/>
</dict>
</plist>
```

These entitlements are required as follows:

- **device.usb** is required because the protected binary may access a USB device (Sentinel HL key).
- **network.client** and **network.server** are required because the protected binary communicates with the Sentinel License Manager (both local and remote) using network sockets
- **allow-unsigned-executable-memory** is required if any application links against (or dynamically loads) dynamic libraries (dylibs) or plug-ins that are protected by Envelope. This is because the code signature is created on the encrypted code section, but the validation occurs after the code is decrypted. Without this entitlement, the validation fails and the protected dylib is not loaded.

This list includes the minimum required entitlements. If your application requires other entitlements, include those also in the file.

2. On the command line prompt, in the terminal, use the **codesign** tool provided with the Apple Developer Tools (Xcode). Enter the following command:

```
yourPath user$ codesign -fv -s "certificateName" -o runtime --timestamp --entitlements
fileName bundleName
```

certificateName is the name of the certificate to be used to sign the bundle. Paste the name that you copied from the Keychain Access Manager. Be sure to enclose the name in double quotation marks.

fileName is the name of the text file create above to contain the entitlements.

bundleName is the name of the bundle to sign.

For example:

```
yourPath user$ codesign -fv -s "Developer ID Application: SFNT Germany GmbH" -o runtime --
timestamp --entitlements my.entitlements Mac_Bounce.app/
```

The system response is similar to this:

```
Mac_Bounce.app/: signed bundle with Mach-O universal (i386 x86_64) [com.safenet-inc.Mac-
Bounce]
```

NOTE To submit a macOS application to the Apple Notary service, you must use the options for hardened runtime, entitlements, and timestamp, as described above and as described in [Resolving Common Notarization Issues](#). You can also find information on the **codesign** man page.

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 to Sentinel LDK v.7.10 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 v.7.10.

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 v.7.10 has been tested only for version 7.6, 7.8, and 7.9. Upgrading from version 7.7 is *not* supported.

NOTE To upgrade from version 7.7, you must first upgrade from 7.7 to 7.8, and then upgrade from 7.8 to 7.10. Version 7.8 is available from: http://d1m.safenet-inc.com/akdlm/ldk/old/LDK_7.8_Windows.zip

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 v.7.10 continues to be supported. For details, see the *Sentinel HASP to Sentinel LDK Migration Guide* provided with Sentinel LDK v.7.10.

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://sentinel.gemalto.com/technical-support/security-updates-sm/>

Reporting a Security Vulnerability

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

<https://sentinel.gemalto.com/technical-support/security-updates-sm/>

Supported Platforms for Sentinel LDK – End Users

The operating system versions listed in this section were tested by Gemalto 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, Gemalto 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 7.100 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*). However, for all pre-existing functionality in Sentinel LDK, earlier versions of the RTE are supported as follows:

> **When using customized vendor API libraries v.7.100 - version-restricted option:**

Whenever the RTE is required, Sentinel LDK Run-time Environment v.7.90 or later must be provided.

> **When using customized vendor API libraries v.7.100 - 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
Windows	<ul style="list-style-type: none"> > 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 Version 1903 <p>Note: Windows 10 Insider Preview builds are not supported. The latest service packs and security updates must be installed.</p>

System	Supported Versions	
Mac	<ul style="list-style-type: none"> > macOS 10.13.6 High Sierra > macOS 10.14 Mojave > macOS 10.15 Catalina (tested with the public beta version) <p>Note: The Sentinel Remote Update System (RUS utility) is not supported for Mac systems in this release. For workarounds, see "End Users, Sentinel LDK Run-time Environment, License Manager, and Customer Tools" on page 35.</p>	
Linux	Linux Intel (x86 and x86-64)	<ul style="list-style-type: none"> > OpenSUSE Leap 15.1 > Red Hat EL 7.6, 8 > Ubuntu Server 16.04, 18.04 > Ubuntu Desktop 18.04 > Debian 10 > CentOS 7.6 <p>The latest service packs and security updates must be installed.</p>
	Linux ARM 32-bit (armel and armhf)	<p>The following hardware/boards have been validated:</p> <ul style="list-style-type: none"> > BeagleBone Black > Raspberry Pi-3 > NI cRIO-9068
	Linux ARM 64-bit (arm64)	<p>The following hardware/board has been validated:</p> <ul style="list-style-type: none"> > Qualcomm DragonBoard 410c
	Wine	<p>Sentinel LDK Run-time Environment was tested on Linux platforms with Wine 4.0.1.</p>

System	Supported Versions	
Android	Android ARM (32-bit and 64-bit)	Android 7.x, 8.x, 9.x
	Android Architecture	The following architectures are supported: <ul style="list-style-type: none"> > armv7 > armv7a > arm64
	Android ABI	Sentinel LDK Envelope supports Android applications designed for the following Android application binary interfaces: <ul style="list-style-type: none"> > armeabi > armeabi-v7a > arm64-v8a
	Note: Data file protection is not supported for Android 7.x and later.	
Virtual Machines	<p>The VM detection and VM fingerprinting capabilities provided by Sentinel LDK have been validated on the following technologies:</p> <ul style="list-style-type: none"> > Parallel Desktop 14 for Mac > VMware Player 6.0.3 (Free for non-commercial use) > VMware Workstation 15 > VMware ESXi 6.5, 6.7 > Hyper-V Server 2019 (SL only) > Xen 4.9 > KVM (RHEL 7.5, Ubuntu 18.04 server, Debian 9.x) > Microsoft Azure > VirtualBox 6.0.x <p>Note: An application that has been protected for performance profiling (with AppOnChip) will not work correctly with earlier versions of Virtual Box.</p> <ul style="list-style-type: none"> > Docker - Linux 	

Data File Protection Plugin for Internet Explorer

The Data File Protection plugin (MSI file) is compatible with the following version of Microsoft Internet Explorer version 11.

NOTE The Data File Protection plugin cannot be installed on a virtual machine.

Web Browsers for Sentinel Admin Control Center

- > Microsoft Internet Explorer (32-bit) version 11

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

Supported Platforms for Sentinel LDK – Vendors

The operating system versions listed in this section were tested by Gemalto 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, Gemalto 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	<ul style="list-style-type: none"> > Windows 7 SP1 > Windows 8.1 SP1 > Windows Server 2008 R2 SP1 > Windows Server 2012 R2 > Windows Server 2016 > Windows Server 2019 > Windows 10 Version 1903 <p>Note: Windows 10 Insider Preview builds are not supported. The latest service packs and security updates must be installed.</p>

Sentinel EMS Database

System	Supported Database Server Software
Windows	<ul style="list-style-type: none"> > Microsoft SQL Server 2014 x86/x64 > Microsoft SQL Server 2014 Express <p>Note: Microsoft SQL Server 2014 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.</p> <ul style="list-style-type: none"> > Microsoft SQL Server 2016 > Microsoft SQL Server 2017 Express

Web Browsers for Sentinel EMS

Supported Browser	Notes
Microsoft Internet Explorer version 11	Some functionality in Sentinel EMS does not work if Sentinel EMS is added to Compatibility View in Internet Explorer.
Mozilla Firefox version 66 or later	RUS customization is not supported with Firefox due to changes in this browser. For details, see "SM-26872" on page 34 .
Google Chrome version 75 or later	RUS customization is not supported with Chrome due to changes in this browser. For details, see "SM-26872" on page 34 .
Microsoft Edge	<p>Certain actions in Sentinel EMS that access protection keys (including burning HL keys and online activation of SL keys) do not work by default in Edge under Windows 32-bit. This is due to a bug in Microsoft Edge. To perform the required actions, you can do one of the following:</p> <ul style="list-style-type: none"> • Use one of the other supported Web browsers. • Enter the command to create an exclusion for Edge on your machine. This enables Edge to work correctly with Sentinel EMS. For details, see "SM-11279" on page 34.

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

For more details regarding supported Web browsers for working in Sentinel EMS with HTTPS mode versus HTTP mode, see "Supported Web Browsers for Sentinel EMS" in the *Sentinel LDK-EMS User Guide*.

Java applets: You must use a 32-bit Web browser for any action in Sentinel EMS that accesses a protection key applet (such as burn, recycle, check in key, or online activation). You can perform all other actions in Sentinel EMS using a 32-bit or 64-bit Web browser.

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	<p>Same as supported Windows platforms for "Sentinel EMS Service" on page 20.</p> <p>Requires a minimum screen resolution of 1280 by 1024 pixels with 24-bit color quality.</p> <p>Note:</p> <ul style="list-style-type: none"> > 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. > Sentinel LDK Master Wizard: Your customized Data File Protection plugin for Internet Explorer (to display certain types of protected multimedia files) is generated when you introduce the Master Key. If you plan to use this plugin, .NET Framework 3.5 or later must be installed on the machine where you run the Master Wizard.
Mac	<ul style="list-style-type: none"> > macOS 10.14 Mojave > macOS 10.15 Catalina (tested with the public beta version) <p>Applications built on the Cocoa framework are supported.</p> <p>Web Browsers for Sentinel Vendor Tools Help Systems:</p> <ul style="list-style-type: none"> > Mozilla Firefox > Mac Safari with configuration option Cross-Origin Restriction disabled. (This option can be accessed from the Developer menu.)
Linux Intel	<p>Sentinel LDK Envelope for Linux and Master Wizard for Linux are supported on the x86 and x86-64 versions of the following distributions of Linux:</p> <ul style="list-style-type: none"> > OpenSUSE Leap 15.1 > Red Hat EL 8 > Ubuntu Server 18.04 > Ubuntu Desktop 18.04 > Debian 10 > CentOS 7.6 <p>The latest service packs and security updates must be installed.</p>
Linux ARM	<p>Sentinel LDK Envelope for Linux (on a Linux Intel platform) is required to protect applications that will run on ARM 32-bit and ARM 64-bit platforms.</p>
Android	<p>Android ARM platforms</p>
Java	<p>Java 8</p>

Supported Platforms for Code Samples

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

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

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

Prior to Sentinel LDK v.7.4, this DLL was compiled with .NET Framework 2.0, which is now known to contain security vulnerabilities. Because of these vulnerabilities, Gemalto 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 XE3
	Java	Oracle Java Developer Kit 1.8
	C# - .NET Core	.NET Core 2.2
	Note: An application linked with libhasp_windows_bcc_vendorld.lib always requires Sentinel LDK Run-time Environment on the machine.	

API	Programming Language	Tested Compilers
Licensing API for Mac OS X	Java	Oracle Java Developer Kit 1.8
	C	Clang 9.0.0 or later Xcode 9.0 or later
Licensing API for Linux	Java	Oracle Java Developer Kit 1.8
	C	GCC
	C++	GCC
	C# - .NET Core	.NET Core 2.2
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
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
Activation API for Mac OS X	Java	Oracle Java Developer Kit 1.8
Activation API for Linux	Java	Oracle Java Developer Kit 1.8
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
	C, C#, C++, Visual Basic .NET	Microsoft Visual Studio 2017, 2019

API	Programming Language	Tested Compilers
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
Android Envelope	Java	Oracle Java Developer Kit 1.7, 1.8 Android Studio 3.1

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
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 v.7.10. Gemalto 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 Software Vendors and End Users

Support for the following platforms has been discontinued:

- > macOS 10.12

> Android 6.x

Dropped Support for 32-bit Linux Vendor Tools

Sentinel LDK Envelope for Linux and Sentinel LDK Master Wizard for Linux are now supported only on 64-bit Linux Intel platforms. Envelope continues to support protection of both 32-bit and 64-bit executables and shared libraries for Linux Intel and Linux ARM.

Dropped Support for 32-bit Applications for Mac

Sentinel LDK no longer supports 32-bit applications for Mac. Both end user components (Run-time Environment and Vlib) and Vendor Tools (Envelope, Data Protection utility, Master Wizard) are only supported for 64-bit.

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://sentinelldk.gemalto.com/Default.htm>

Documents

Sentinel LDK documents (PDF files) can be found:

- > on the (physical) Sentinel LDK Installation Drive, under: **\\Windows\\Installed\\Docs**
- > where Sentinel LDK is installed, under:
%ProgramFiles(x86)%\\Gemalto Sentinel\\Sentinel LDK\\Docs
- > where Sentinel EMS is installed, under:
%ProgramFiles(x86)%\\Gemalto Sentinel\\Sentinel EMS\\EMSServer\\webapps\\ems\\Docs
 (For Win32, under: **%ProgramFiles%\\...**)

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	<p>Familiarize you with the Sentinel LDK applications and their functionality.</p> <ul style="list-style-type: none"> > The Demo Kit tutorial is for vendors that want to evaluate Sentinel LDK. > The Starter Kit tutorial is for vendors that have already purchased Sentinel LDK. <p>Two versions of each tutorial are provided – one for working with Sentinel EMS as the back office system, and one for vendors who want to provide their own back office system and only use the Sentinel LDK APIs to handle licensing and protection.</p>
Sentinel LDK Quick Start 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.
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.
Additional Guides for Migrating to Sentinel LDK	<p>These guides describe how to migrate to Sentinel LDK from:</p> <ul style="list-style-type: none"> > Hardlock > SmartKey > Sentinel SuperPro > HASP HL > HASP4 > Sentinel Hardware Keys
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.
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.

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 on the Sentinel LDK Installation Drive, under: **\Linux**

macOS

The *Getting Started Guide for macOS* can be found in the Mac download or on the Sentinel LDK Installation Drive, under: **\MacOS**

Android

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

- > on the (physical) Sentinel LDK Installation Drive, under: **\Android**
- > where Sentinel LDK is installed, under:
%ProgramFiles(x86)%\Gemalto Sentinel\Sentinel LDK\Additional Platforms\Android
 (For Win32, under: **%ProgramFiles%\...**)

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.
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.

Online Help System	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.

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://sentinelldk.gemalto.com/Default.htm>
- > on the Sentinel LDK Installation Drive, under: **\\Windows\\Installed\\API**
- > where Sentinel LDK is installed, under:
%ProgramFiles(x86)%\\Gemalto Sentinel\\Sentinel LDK\\API
(For Win32, under: **%ProgramFiles%\\...**)

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.
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)%\\Gemalto Sentinel\\Sentinel EMS\\EMSServer\\webapps\\ems\\Docs\\ (For Win32, under %ProgramFiles%\\...)

Sentinel LDK API	Description
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

Gemalto 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 described issues that were reported by vendors and that have been resolved in this release of Sentinel LDK.

Reference	Resolved Issue	Components
SM-38151 SM-27435	A customer was not able to use Data File Protection (Version 2) for the customer's Windows application.	Envelope Data File Protection
SM-45401 SM-44489	A protected application would fail due to a segmentation fault with Envelope 7.9 ELF AMD64.	Envelope (Linux)
SM-45412 SM-44229	For certain application that were protected with default Envelope settings, the protected application would not run.	Envelope
SM-45103 SM-44014	A problem occurred with ResXFileCodeGenerator when moving from Envelope 7.5 to Envelope 7.8.	Envelope (.NET)
SM-43953 SM-43327	Internal error "0x7101" would occur if the customer's application was protected using program number.	Envelope

Reference	Resolved Issue	Components
SM-43952 SM-41821	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> > A .NET application was protected by Windows shell protection > The application was started from a folder that is different from the folder that contains the executable file <p>The current working directory was changed to the folder that contains the executable file. This may affect the behavior of the original application.</p>	Envelope
SM-41870 SM-45384 SM-41172	For a specific JAR, Data File Protection was not working correctly with Envelope on Java.exe.	Envelope Data File Protection
SM-56547 SM-56365	During protection, the trailing zeros for a static string of numbers were stripped.	Envelope (.NET)
SM-57072 SM-51459	Envelope.com would hang after a certain number of iterations.	Envelope
SM-53801 SM-52305	For a protected application on a 64-bit machine, .NET DLL would crash.	Envelope (.NET)
SM-55400	The Vendor Code file would not be loaded correctly when the name of the path that contains the file contained a special character.	Envelope
SM-50180 SM-50001	<p>When decrypting and decompressing an encrypted and compressed resource file, the following messages was generated:</p> <p>System.IO.InvalidDataException: The magic number in GZip header is not correct. Make sure you are passing in a GZip stream.</p>	Envelope (.NET)
SM-47607 SM-35431 SM-48569	Under macOS 10.14, Envelope would not launch. macOS would generate an alert that the binary was downloaded and it cannot be started. This issue would only occur when the software is downloaded from the internet.	Envelope (Mac)
SM-48047 SM-43553	<p>An application protected with Envelope for Linux 7.6 or 7.8 would generate a “Bus error” when launched under the following conditions:</p> <ul style="list-style-type: none"> > The "protocolbuffer" library is included in the project. > The iMX6 board is used. 	Envelope (Linux ARM)
SM-47474 SM-47345	When protecting a certain application with “Disable key for attempted tampering” selected, Envelope would generate the message: The option Disable key for attempted tampering is not selected.	Envelope

Reference	Resolved Issue	Components
SM-24207 SM-43162 SM-34673 SM-18929 SM-47046	Envelope would not support Multiple Thread Local Storage variable for shared libraries on the Linux ARM 64-bit platform. Envelope would return SEGMENTATION FAULT when protecting the application.	Envelope (Linux ARM)
SM-23850 SM-23411 SM-37558	In certain scenarios, Envelope would crash when switching between several .NET sample applications.	Envelope
SM-52601 SM-51703	Under certain circumstances data protected with Version 1 data file protection worked correctly, but data protected with Version 2 data file protection could not be decrypted.	Data File Protection
SM-48915 SM-49171 SM-48562	Under Linux, if a protected application opened two protected data files at the same time, the first file was decrypted, but the second file was not decrypted correctly.	Envelope Data File Protection Envelope (Linux)
SM-54726 SM-53853 SM-53715	A protected application would crash when unloading the DLL when the "Application Verifier" memory leak test is enabled.	Envelope RunTime/API

Known Issues and Workarounds

The known issues in Sentinel LDK v.7.10 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	<p>Installation of Sentinel LDK on a virtual machine may hang before completion of the installation process.</p> <p>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.</p>

Ref	Issue
EMSLDK-7448	<p>Sentinel EMS fails to install correctly on a machine where JRE 8 and earlier versions of JRE coexists.</p> <p>If a machine contains an earlier version of JRE, and you manually install JRE 8, then:</p> <ul style="list-style-type: none"> > 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. <p>This occurs because while upgrading to JRE 8 , the Java installer does not replace earlier JRE files from the System32 directory.</p> <p>Workaround: Uninstall the earlier versions of JRE from your machine, and restart the Sentinel EMS installation.</p> <p>Note:</p> <ul style="list-style-type: none"> > 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.
SM-35287	<p>When upgrading from Sentinel LDK v.7.3 through v.7.8 to Sentinel LDK v.7.10, all non-English locales of Customer contacts and Channel Partner contacts in Sentinel EMS are converted to the English locale.</p> <p>Note: You can ignore this issue if all of your Customer and Channel Partner contacts are set up to use the English locale or if you are not upgrading Sentinel EMS.</p> <p>Workaround: A solution for this issue is provided in the technical note available here.</p>

Sentinel EMS

Ref	Issue
SM-11279	<p>Certain actions in Sentinel EMS that access protection keys (including burning HL keys and online activation of SL keys) do not work by default in Edge under Windows 32-bit. This issue is caused by a bug in Microsoft Edge. For details, see: https://developer.microsoft.com/en-us/microsoft-edge/platform/issues/10082889/</p> <p>Workaround: Create an exclusion for Edge to allow localhost loopback as follows:</p> <ol style="list-style-type: none"> 1. Move the cursor to the bottom-left corner of your screen, and right-click the Windows icon. 2. In the resulting menu, select Command Prompt (Admin). The Command Prompt (Admin) window is displayed. 3. Copy and paste the following command to the Command Prompt window, and press Enter: <pre>CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"</pre> <p>Edge will now work correctly with Sentinel EMS.</p>
SM-12832	<p>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.</p> <p>Workaround: In the etc/host file on the user's machine, add an entry that contains the hostname and IP address of the Sentinel EMS machine.</p>
SM-19045	<p>Customers who were associated with a channel partner prior to Sentinel LDK 7.7 will not be visible in Sentinel EMS to the relevant Channel Partner user. However, the Channel Partner user will not be able create a new entry for an existing customer with the same email address as already exists in the EMS database. In this situation, the Channel Partner user will not be able to fulfill an entitlement for the customer.</p> <p>Workaround: If the Channel Partner user cannot create the required customer in Sentinel EMS, the software vendor should handle the fulfillment of the entitlement for the customer.</p>
SM-26872	<p>When working with Firefox version 57.0.3 or later or with Chrome, you cannot provide custom text while creating a branded version of the RUS utility from the RUS Branding tab in Sentinel EMS.</p> <p>Workaround: Use Internet Explorer 11. This will allow you to provide text while creating a branded version of the RUS utility.</p>
SM-52262	<p>After you introduce or update a Master Key, you must notify all Sentinel LDK-EMS users to log off and log on again to get the latest changes.</p>

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

Ref	Issue
	<p>The Sentinel Remote Update System (RUS utility) is not supported for Mac systems in this release.</p> <p>Workaround: To obtain a fingerprint, use the Licensing API sample (hasp_update). Alternatively, install an unlocked license, fetch its C2V using Admin Control Center, and use that to generate a license.</p>
LDK-8480	<p>With some new USB chipsets, it is possible that the hasp_update() API call, used to update the firmware of Sentinel HL keys to version 3.25, will generate the HASP_BROKEN_SESSION return code, even if the firmware is correctly updated. (This issue does not occur with Sentinel HL Driverless keys with firmware version 4.x.)</p> <p>Workaround: Install the latest Run-time Environment. The automatic firmware update feature of the License Manager will automatically update the firmware of the key the first time that the key is connected, without the need to call hasp_update().</p>
LDK-9044	<p>Given the following circumstances:</p> <p style="padding-left: 40px;">A Sentinel HL (Driverless configuration) key is connected to a USB host controller in default mode on QEMU emulator version 2.0.0 and Virtual Machine Manager version 0.9.5.</p> <p>When the key is disconnected, the key continues to be displayed in Admin Control Center as a connected key. (However, a protected application whose license is located in the key does not execute after the key is disconnected.)</p> <p>Workaround: Switch the USB controller to USB 2.0 mode.</p>
LDK-10670	<p>After a user connects a Razer Abyssus mouse and installs Razer drivers on a computer, the device manager on the computer does not recognize a Sentinel HL key if the key is connected to the same USB port where the mouse was previously connected.</p> <p>This issue has been reported to Razer.</p>
LDK-12172	<p>The Data File Protection plugin is installed in both 32-bit and 64-bit Internet Explorer. However, the plugin is not functional in 64-bit Internet Explorer.</p> <p>Workaround: Use the 32-bit Internet Explorer to view protected data files.</p>
LDK-12547	<p>Under Linux, if the user is running a Windows 64-bit protected application using Wine with default options, Linux may return a "debugger detected" error.</p> <p>Workaround: When you protect the application using Envelope, disable User debugger detection for the application. (Note that disabling debugger detection reduces the overall security of the application.)</p>

Ref	Issue
LDK-14971	<p>Given the following circumstances at a customer site:</p> <ul style="list-style-type: none"> > One machine has Run-time Environment version 7.51. > A second machine has a version of Run-time Environment that is earlier than v.7.51. > The customer performs rehost of a license repeatedly between the two machines. > An update is applied to the license on either of these machines. <p>A rehost operation may fail with the message HASP_REHOST_ALREADY_APPLIED.</p> <p>Workaround: Obtain a new SL license from the software vendor for the protected application on the target machine. Before attempting any additional rehost procedure, install the latest Run-time Environment on both machines.</p>
LDK-15991	<p>When working in Internet Explorer with Enable Protected Mode selected and with Enable Enhanced Protected Mode selected, the Data File Protection plugin cannot open encrypted flv/swf/mp4 files because the plugin cannot locate the license. If only Enable Protected Mode is enabled, the plugin cannot locate an SL UserMode license.</p> <p>Workaround: Start Internet Explorer as an administrator. The Data File Protection plugin will locate any type of license regardless of the state of Protected Mode and Enhanced Protected Mode.</p>
SM-546	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> > A protected application was created using Visual Studio 2015 > Control Flow Guard is explicitly enabled in Visual Studio. > The application links statically or dynamically with Sentinel Licensing API. > The External License Manager (hasp_rt.exe) is not used. > The application is run under Windows 10, or Windows 8.1 Update (KB3000850). (Not all Windows 8.1, only recent ones) <p>The protected application may fail.</p> <p>Workaround: Include the External License Manager (hasp_rt.exe) with the protected application.</p>
SM-10843	<p>The FLV player (flvplayer.swf) under %ProgramFiles(x86)%\Gemalto Sentinel\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:</p> <ul style="list-style-type: none"> > 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-59868	<p>An application linked with libhasp_windows_bcc_vendorId.lib requires Sentinel LDK Run-time Environment on the machine.</p>

Sentinel LDK Envelope and Data Encryption for Windows Platforms

General

Ref	Issue
LDK-11727	<p>Debugger detection is not provided for .NET applications.</p> <p>Workaround: Implement debugger detection mechanism in the application code, and use Envelope to protect the methods that call these functions.</p>
LDK-11191	<p>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.</p>
LDK-6695	<p>When a "Debugger Detected" error is generated, it is not possible for the protected application to determine which process is regarded as a debugger.</p>
LDK-8850	<p>When a protected application detects that a debugger is attached, the application may generate multiple "Debugger Detected" message windows.</p>
SM-58676	<p>Given the following circumstances:</p> <ol style="list-style-type: none"> 1. Install SL AdminMode licenses on your local machine. 2. Run IObit Advanced SystemCare Ultimate 12 to clean and optimize your machine. 3. Restart your machine. <p>Local SL AdminMode licenses may be missing or may be identified as cloned licenses. This is an issue with the IObit product. Gemalto has reported this issue to IObit and it is currently under investigation.</p> <p>Workaround: Do not use the current version of the IObit product, <i>OR</i> do not use SL AdminMode licenses until this issue is resolved. (You can use SL UserMode licenses.)</p>
SM-65381	<p>Under Windows, execution of a Python application that is protected with DFP sometimes fails with the "Bad magic number" error if hasp_rt.exe is not present in the protected folder.</p> <p>Workaround: Ensure that hasp_rt.exe is present in the protected folder.</p>

Java

Ref	Issue
LDK-11195	<p>When protecting a Java application, Envelope fails with the message "Serious Internal Error (12)".</p> <p>Workaround: If this error occurs, protect the Java application using either of the following techniques:</p> <ul style="list-style-type: none"> > If the application contains JARs within a JAR/WAR executable, remove those JARs when protecting the executable with Envelope. You can add the JARs to the JAR/WAR executable after protection is complete. > Create a JAR/WAR executable using only those classes that you want to protect. After applying protection, you can add other classes or JARs, or any other dependencies in the protected JAR/WAR executable.
LDK-11418	<p>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:</p> <ul style="list-style-type: none"> > Java 7: Specify <code>java -UseSplitVerifier -jar ProtectedJar.jar</code> > Java 8: Specify <code>java -noverify -jar ProtectedJar.jar</code> <p>If the appropriate flag is not specified, the application may throw java.verifyerror when launched.</p>
SM-10890	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> > An Envelope project was created with Envelope version 7.3 or earlier. > The project contains settings for a Java application. > On the Protection Settings tabbed page for the Java application, you select the option to overwrite default protection settings. <p>The Allows grace period after failed license check check box should be modifiable. However, the check box cannot be changed.</p> <p>Workaround: On the Advanced tabbed page, make any change to the MESSAGE_OUTPUT_MODE property, and then change it back. This forces Envelope to load an internal data structure that then makes the Allows grace period after failed license check check box modifiable.</p>
SM-10969	<p>Due to a known limitation in Java, if a background check thread becomes non-EDT, the background check (Abort/Retry/Ignore) dialog box may not appear. Envelope has been modified so that the error dialog prompted by the protected method in the protected application takes precedence. This has reduced the occurrence of the problem, but it has not eliminated the problem entirely.</p>

.NET

Ref	Issue
SM-554	<p>For apps that target the .NET Framework version 4.6 and later, CultureInfo.CurrentCulture and CultureInfo.CurrentUICulture are stored in a thread's ExecutionContext, which flows across asynchronous operations. As a result, changes to the CultureInfo.CurrentCulture and CultureInfo.CurrentUICulture properties are reflected in asynchronous tasks that are launched subsequently.</p> <p>If the current culture or current UI culture differs from the system culture, the current culture crosses thread boundaries and becomes the current culture of the thread pool thread that is executing an asynchronous operation.</p> <p>When protecting a sample application implementing above behavior with protection type as "Dot Net Only", then the application behaves as expected. However, with protection type "Dot Net and Windows Shell" or "Windows Shell Only", the thread uses the system's culture to define behavior.</p> <p>Workaround: Do the following:</p> <ol style="list-style-type: none"> 1. Use .NET Framework 4.5. 2. Use <pre>CultureInfo.DefaultThreadCurrentCulture = new CultureInfo(...)</pre> instead of <pre>Thread.CurrentThread.CurrentCulture = new CultureInfo(...).</pre>
SM-25875	<p>Given the following circumstances:</p> <ol style="list-style-type: none"> 1. A .NET application is protected with Envelope. 2. The protection type includes Windows Shell (with or without the method level). 3. The application attempts to get a module handle using the following method: <pre>IntPtr hMod = Marshal.GetHINSTANCE(Assembly.GetExecutingAssembly() ().GetModules()[0])</pre> <p>The handle returned may not be correct, and as a result, an error will be generated.</p> <p>Workaround: You can call the GetModuleHandle system API of the Kernel32.dll to get the module handle.</p> <p>For example:</p> <pre>[DllImport("kernel32.dll", CallingConvention = CallingConvention.StdCall, CharSet = CharSet.Auto)] private static extern IntPtr GetModuleHandle(IntPtr lpModuleName); IntPtr hMod = GetModuleHandle(Process.GetCurrentProcess ().MainModule.ModuleName);</pre>
SM-26578	<p>If a .NET application protected with Windows Shell sets the exit code to ExitEventArgs such as "e.ApplicationExitCode = 1" when the application exits, the exit code cannot be retrieved by an external process.</p> <p>Workaround: Call "Environment.Exit(1)" to exit the process.</p>

Android

Ref	Issue
SM-38233	Data File Protection is not currently supported for Android 7 and later devices.

Sentinel LDK Envelope and Data Encryption for Linux

Ref	Issue
SM-24207	For Linux ARM 64-bit platforms, Envelope does not protect a shared library that uses multiple thread local storage variables. Envelope may return a SEGMENTATION FAULT error when attempting to protect such a shared library or may fail during execution of the protected shared library.

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

Ref	Issue
LDK-11655	<ul style="list-style-type: none"> > When running Envelope in a VMware Fusion 7.1.1 virtual machine on a Mac machine, if you save the protected application to an HGFS (Host Guest File System) volume, the application file is corrupted. > When you run a protected application on a VMware Fusion virtual machine from an HGFS share, if the application requires write access, the error "unable to write to file" is generated.
SM-57838	The command line Envelope tool (envelope_darwin) now only works if Envelope.app (UI bundle) is in the same folder. To use the command line tool, copy Envelope.app to the folder that contains the command line tool.
SM-57024	Dark Mode has been introduced by Apple in macOS 10.14 but is not supported yet by the Envelope GUI. You should disable Dark Mode to have a proper user experience.
SM-51456	<p>Due to reliability enhancements in Sentinel LDK under macOS, there is some performance impact in protected applications under macOS 10.13.</p> <p>A technical note will be issued in August 2019 that describes this issue and the option to disable these enhancements in favor of higher performance.</p>

Sentinel LDK Envelope for Android

Ref	Issue
SM-57733	<p>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.</p> <p>Workaround: Gemalto 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:</p> <ol style="list-style-type: none">1. Protect the application using Licensing API.2. Remove one RUS from the APK file.3. Protect the application with Envelope.