

Sentinel LDK – v.7.9

Release Notes

Revision History

Part number 007-013811-003, Rev A

Copyrights and Trademarks

© Gemalto 2019. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

HARDLOCK, HASP, SENTINEL, SUPERPRO and ULTRAPRO are registered trademarks of SafeNet, Inc. and/or its subsidiaries and may not be used without written permission.

All other trademarks are property of their respective owners.

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.

December 2018 Revision 1901-3

Contents

Sentinel LDK v.7.9 - Release Notes	5
About This Document	5
Product Overview	5
Sentinel Vendor Keys	6
Obtaining Support	6
What's New in Sentinel LDK v.7.9?	7
Custom Clone Protection Schemes	7
Sentinel LDK Now Supports Data File Protection for Linux Platforms	7
Sentinel LDK Envelope User Interface Has Been Improved	8
Program Integrity Protection Feature Has Been Added to Sentinel LDK Envelope for Windows	8
Sentinel LDK Now Supports Android 8 and 9	8
Software Manager System Upgraded to Sentinel Up	8
What's Changed in Sentinel LDK v.7.9?	9
Sentinel EMS Web Services Have Been Modified to Protect Against Verb Tampering	9
Legacy Components of Sentinel LDK Have Been Removed	9
Parameter to Allow Remote Access in License Manager Has Been Split	10
Samples for Android Envelope and for Runtime API Now Requires Android Studio	10
Correction to Software Protection and Licensing Guide	11
Upgrading From an Earlier Version of Sentinel LDK	11
Security Updates	11
Reporting a Security Vulnerability	12
Supported Platforms for Sentinel LDK – End Users and Vendors	12
Supported Platforms for End Users	12
Supported Platforms for Vendors	15
Supported Platforms for Code Samples	17
Tested Compilers for Code Samples	18
Current Firmware Version	19
Dropped Support	20
Platforms for Software Vendors and End Users	20
Compilers	20
Sentinel Components	20
Planned Drop of Support	20
Sentinel LDK Documentation	20
Documents	21
Getting Started Guides	22
Help Systems - Sentinel LDK and Sentinel EMS User Interfaces	23
Online Help Systems – Sentinel LDK APIs	23
Instructional Videos	24
Software and Documentation Updates	24

Known Issues and Workarounds	25
Sentinel LDK Installation	25
Sentinel EMS	26
End Users, Sentinel LDK Runtime Environment, License Manager, and Customer Tools ...	27
Sentinel LDK Envelope and Data Encryption for Windows Platforms	29
Sentinel LDK Envelope and Data Encryption for Linux	32
Sentinel LDK Envelope and Data Encryption for Mac OS X	32

Sentinel LDK v.7.9 - 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 release of Sentinel LDK 7.9 as follows:

- The release notes now state that Sentinel LDK Run-time Environment, Sentinel Vendor Tools, and protected applications are supported under Windows Server 2019.
- The release notes now state that Sentinel LDK Run-time Environment and protected applications are supported under Windows 10 IoT Enterprise 2016.



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 from the Sentinel Community web site to see if any information was added or changed. You can access the latest release notes from this location:

http://sentinelcustomer.gemalto.com/Documentation_Information.aspx

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. The 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 only allow trusted personnel to use them. The Master key is especially valuable because it allows the generation of 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.7.9?

This section describes the main features and enhancements that are introduced in this release of Sentinel LDK.



If you are upgrading from a version of Sentinel LDK that is earlier than v.7.8, 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 from the Sentinel Customer Community download page.

Custom Clone Protection Schemes

Sentinel LDK now allows you to specify custom clone protection schemes for your Product licenses. When defining a Product, you can create a named clone protection scheme and assign it to the Product. The named scheme is also available to assign to other Products.

Separate clone protection schemes can be specified for physical machines and for virtual machines.

For each custom clone protection scheme, you select the criteria to use from a list. You also specify how many of the selected criteria must be satisfied in order for the License Manager to validate the license.

Custom clone protection schemes can be specified using either the Sentinel EMS web interface or Sentinel License Generation API. (Custom clone protection schemes are not currently supported for Sentinel EMS Web Services.)

Custom clone protection schemes are supported for SL AdminMode and SL UserMode keys. For SL AdminMode keys, Sentinel LDK Run-time Environment version 7.90 or later must be present on the computer where the protected application executes.

Sentinel LDK Now Supports Data File Protection for Linux Platforms

You can now use Sentinel LDK Envelope for Linux to add the Data Protection module to a protected application. (For Linux applications, only the **Version 2** data protection mode is

supported.) This enables the protected application to access a protected data file when the protection key contains the appropriate license for the data file. (Update of a protected data file is not currently supported.)

Sentinel LDK Envelope for Linux operates only under Linux Intel; however, it can protect applications for both Linux Intel and Linux ARM platforms. You protect the data files using Sentinel LDK Data Protection utility, operating under Windows.

To operate Sentinel LDK Data Protection utility with the Version 2 protection mode, you must connect a Sentinel Master key or Developer key with the Advanced Data File Protection module to your machine.

For more information, see the description of data file protection in the *Sentinel LDK Software Protection and Licensing Guide*.

Sentinel LDK Envelope User Interface Has Been Improved

The Sentinel LDK Envelope graphical user interface has been modified to provide better control of the class/method tree in .NET and Java. Settings that are not commonly used have been moved to allow more space for the class/method tree. The process for selecting classes and methods has been improved.

Program Integrity Protection Feature Has Been Added to Sentinel LDK Envelope for Windows

The option **Program integrity protection** is now available in the protection settings for Windows applications. When this option is selected, the protected application is signed with a digital signature. At run-time, the signature is checked to ensure that the code was not modified.

Program integrity protection is compatible with Microsoft Authenticode signatures. It is possible to apply a Microsoft Authenticode signature to the protected application when the **Program integrity protection** option is selected.

(This feature was already present for .NET assemblies in Sentinel LDK v.7.8.)

Sentinel LDK Now Supports Android 8 and 9

Sentinel LDK now supports Android 8 and 9, including the Licensing API and Envelope. 64-bit ARM is also supported, including the Licensing API, samples, and flows related to license updates.

(Support for Android 64-bit ARM was provided initially in Sentinel Run-time Environment version 7.81.)

Software Manager System Upgraded to Sentinel Up

The system used to deliver online updates to Sentinel LDK components has been switched to Gemalto's **Sentinel Up**. This software manager system provides improved reliability for the delivery of future updates to Sentinel LDK on the vendor's machine.

What's Changed in Sentinel LDK v.7.9?

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

Sentinel EMS Web Services Have Been Modified to Protect Against Verb Tampering

HTTP verb tampering is an attack that exploits HTTP verb-based authentication and access control mechanisms. The vulnerability lies in the configuration of the security constraints that specify HTTP verbs that often allow more access than intended.

An application's authentication and authorization mechanisms can be bypassed with HTTP verb tampering when the security control fails to block verbs that are not listed.

In this release, Sentinel EMS Web Services were modified to prevent HTTP verb tampering. The methods that are used by Web Services have been whitelisted: GET, POST, DELETE, PUT. When calling these methods in your application, you must ensure that they are written using only upper-case letters as shown here. Variations that used lower-case or mixed-case letters have been blocked.

This is a standard practice as suggested by the Internet community and is mentioned in RFC standard protocols (RFC 7230 and 7231).

Gemalto recommends that you review any application that calls Sentinel EMS Web Services to ensure that you are calling methods following the practices described above. The use of method calls that do not comply with these practices will cause your application to fail (error code 403).

Legacy Components of Sentinel LDK Have Been Removed

The table below describes components of Sentinel LDK that have been removed for this release.

Component	Notes
\Windows\Installed\Runtime Environment	Run-time Environment files related to Windows XP Embedded (which is no longer supported by Microsoft). As a result, <i>%ProgramFiles(x86)%\Gemalto Sentinel\Sentinel LDK\Runtime Environment</i> is no longer installed.
\Windows\Installed\Legacy\API\Activation	Replaced by more advanced Activation API. See the Samples\Activation folder.
\Windows\Installed\Legacy\Samples	Legacy Activation sample has been removed.
\MacOS\Legacy	Legacy Activation API and sample have been removed. These have been replaced by a more advanced Activation API. See the Samples\Activation folder.
\Linux\Legacy	

Parameter to Allow Remote Access in License Manager Has Been Split

The parameters described below configure the License Manager on a given machine to allow or deny access to the local Admin Control Center (ACC) or Admin API from a remote machine.

Facility	Parameter/Tag	Description
Admin Control Center	Allow Remote Access to ACC and Admin API	When selected or enabled, enables other network users to access and perform actions in Admin Control Center and Sentinel Admin API on this machine.
Admin API	<accremote>	Unselected/disabled by default.

In each case, a single parameter controls remote access whether the user is attempting to access the local Admin License Manager using either Admin Control Center or Admin API.

In the License Managers for Sentinel LDK 7.9, these parameters have been split to provide more granular control of access from a remote machine. You can now allow or deny access separately for Admin Control Center and for Admin API.

The following parameters are now provided.

Facility	Parameter/Tag	Description
Admin Control Center	Allow Remote Access to ACC	When selected or enabled, allows remote network users to access and perform actions in Admin License Manager using Admin Control Center on this machine.
Admin API	<accremote>	Unselected/disabled by default.
Admin Control Center	Allow Remote Access to Admin API	When selected or enabled, allows remote network users to access and perform actions in Admin License Manager using Admin API on this machine.
Admin API	<adminremote>	Unselected/disabled by default.

When the License Manager is upgraded to version 7.90, each new parameter is assigned the value that was assigned to the original parameter. As a result, after the upgrade, there is no change in access granted.

Samples for Android Envelope and for Runtime API Now Requires Android Studio

The Eclipse ADT samples for Android Envelope and for Runtime API that were provided in earlier releases of Sentinel LDK are no longer supported. To support Android 8 and later, the samples provided for Sentinel LDK Android Envelope and for Runtime API require Android Studio.

Correction to Software Protection and Licensing Guide

The Sentinel LDK Software Protection and Licensing Guide has been corrected by the addition of the note that follows.

You can create a Product with no Features whose only purpose is to define protection key memory. For this type of Product, the restriction below applies.

If both of the following conditions exist:



- The protected application can be used on a virtual machine.
- The Product may reside in an SL key.

The Product must include a dummy Feature that is enabled for virtual machines. Otherwise, the application will not operate on a virtual machine when the application is licensed with an SL key.

This note is applicable for Sentinel LDK v.7.4 and later.

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, described in "[Sentinel LDK Documentation](#)" on page 20.

Note the following issues:

- When upgrading from Sentinel LDK v.7.3 through v.7.8 to Sentinel LDK v.7.9, 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 7.9.
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.7.9 has only been tested for Sentinel LDK versions 7.6 through 7.8.

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.7.9 continues to be supported. For more information, see the *Sentinel HASP to Sentinel LDK Migration Guide*, provided with Sentinel LDK v.7.9.

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 this Web page:

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

Reporting a Security Vulnerability

If you think you have found a security vulnerability, please send it to Gemalto using the links provided on the Web page provided above.

Supported Platforms for Sentinel LDK - End Users and 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 fully 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.

Supported Platforms for End Users

Sentinel LDK Run-time Environment, Protected Applications

The following Sentinel LDK Run-time Environments are provided with this release of Sentinel LDK:

System	Run-time Environment Version
Windows	Version 7.90
Mac	Version 7.90
Linux Intel	Version 7.90



To support all the latest enhancements in Sentinel LDK, end users should be provided with the latest Run-time Environment. However, for all pre-existing functionality in Sentinel LDK, respective earlier versions of Sentinel Run-time Environment are supported except as noted below.



Sentinel Run-time Environment version 7.90 or later is required when both of the following conditions exist:

- The protected application uses Sentinel Licensing API version 7.9 or later.
- The protection key used by the application requires the presence of the Run-time Environment.

The 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 2016 ■ Windows 10 Version 1809 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Windows 10 Insider Preview builds are not supported. </div> <p>The latest service packs and security updates must be installed.</p>	
Mac	<ul style="list-style-type: none"> ■ macOS 10.12 ■ macOS 10.13.6 (High Sierra) ■ macOS 10.14 (Mojave) <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  The Sentinel Remote Update System (RUS utility) is not supported for Mac systems in this release. For workarounds, see "End Users, Sentinel LDK Runtime Environment, License Manager, and Customer Tools" on page 27. </div>	
Linux	Linux Intel (x86 and x86-64)	<ul style="list-style-type: none"> ■ OpenSUSE Leap 15.0 ■ Red Hat EL 6.9, 7.5 ■ Ubuntu Server 16.04, 18.04 ■ Ubuntu Desktop 18.04 ■ Debian 9 ■ CentOS 7.5 <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"> ■ BeagleBoard-xM Rev C ■ BeagleBone Black ■ Raspberry Pi-2, Pi-3 ■ PandaBoard ES Rev B3_ ■ NI cRIO-9068
	Linux ARM 64-bit (arm64)	<p>The following hardware/board has been validated:</p> <ul style="list-style-type: none"> ■ Qualcomm DragonBoard 410c
	Wine	Sentinel LDK Run-time Environment was tested on Linux platforms with Wine 3.0.3.

System	Supported Versions	
Android	Android ARM (32-bit and 64-bit)	Android 6.x, 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 supported only for Android 6.x with the armv7a architecture.	
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 14 ■ VMware ESXi 5.5, 6.0 ■ Hyper-V Server 2016 ■ Xen 4.6 ■ KVM (RHEL 7.5, Ubuntu 18.04 server, Debian 9.x) ■ Microsoft Azure ■ VirtualBox 5.2.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> <p>For Docker support, see public article KB0018118.</p>	

Data File Protection Plugin for Internet Explorer

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

- Versions 8 through 11.



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 Vendors

Sentinel EMS Service


System	Supported Versions
Windows	See supported Windows platforms for Sentinel LDK Run-time Environment (above).

Sentinel EMS Database

System	Supported Database Server Software
Windows	<ul style="list-style-type: none"> ■ Microsoft SQL Server 2012 x86/x64 <div data-bbox="451 972 1393 1062" style="border: 1px solid black; padding: 5px; margin: 5px 0;">  For detailed instructions on how to install and configure SQL Server 2012 for Sentinel EMS, see the Technical Note available here. </div> ■ Microsoft SQL Server 2014 x86/x64 ■ Microsoft SQL Server 2014 Express <p>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 DVD.</p> ■ Microsoft SQL Server 2016

Web Browsers for Sentinel EMS

- Microsoft Internet Explorer version 11
- Mozilla Firefox version 62 or later
- Google Chrome version 69 or later

 RUS customization is not supported with Firefox or Chrome due to changes in these browsers. For more information, see "[SM-26872](#)" on page 26.

- Microsoft Edge

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:



- 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 more information see "[SM-11279](#)" on page 26.



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

For more detailed information regarding supported Web browsers for working in Sentinel EMS with HTTPS mode versus HTTP mode, see section 1.2.3, "Supported web Browsers for Sentinel EMS" in the *Sentinel EMS User Guide*.

For situations where Java applets are used: 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

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 1809 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Windows 10 Insider Preview builds are not supported. </div> <p>The latest service packs and security updates must be installed. Requires screen resolution 1280 by 1024 pixels with 24-bit color quality</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> 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. </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> For 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 present on the machine where you run the Master Wizard. </div>

System	Supported Versions
Mac	<ul style="list-style-type: none"> ■ macOS 10.13.6 High Sierra ■ macOS 10.14 High Sierra (64-bit mode is not supported) <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
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 15.0 ■ Red Hat EL 7.5 ■ Ubuntu Server 18.04 ■ Ubuntu Desktop 18.04 ■ Debian 9.x (x86 and x86_64) ■ CentOS 7.5 <p>The latest service packs and security updates must be installed.</p>
Linux ARM	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 (MIPS platform is not supported.)
Java	Java 8

Supported Platforms for Code Samples

Provided code samples are supported on the same platforms as listed above for Sentinel LDK Vendor Tools.

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. Prior to Sentinel LDK v.7.4, this DLL was compiled with .NET Framework 2.0. As a result, vendors who want to work with the provided DLL must upgrade to .NET Framework 4.5 or later.



Gemalto made this change because .NET Framework 2.0 contains known 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 Customer Support.

Tested Compilers for Code Samples

API	Programming Language	Tested Compilers
Licensing API for Windows	AutoCAD	AutoCAD 2009, 2010, 2014
	C	Microsoft Visual Studio 2013, 2015, 2017 C++ Builder Developer Studio 2006
	Visual Basic .NET	Microsoft Visual Studio 2015, 2017
	C#	Microsoft Visual Studio 2015, 2017
	C++	Microsoft Visual Studio 2013, 2015, 2017 C++ Builder Developer Studio 2006 GCC
	Delphi	Developer Studio 2006 Delphi XE3
	Java	Java Developer Kit 1.8
Licensing API for Mac OS X	Java	Java Developer Kit 1.8
	C	Clang, Xcode x.x
Licensing API for Linux	Java	Java Developer Kit 1.8
	C	GCC
	C++	GCC
Licensing API for Android	Java	Java Developer Kit 1.8
License Generation API	C, C#, Visual Basic .NET	Microsoft Visual Studio 2015, 2017
	Java	Java Developer Kit 1.8
Activation API for Windows	C	Microsoft Visual Studio 2013, 2015, 2017 You may need to convert the provided workspace for the VS version used.
	Java	Java Developer Kit 1.8
Activation API for Mac OS X	Java	Java Developer Kit 1.8
Activation API for Linux	Java	Java Developer Kit 1.8
Runtime Environment Installer	C	Microsoft Visual Studio 2013, 2015, 2017
	MSI	InstallShield 12 InstallShield 2013

API	Programming Language	Tested Compilers
Admin API for Windows	Java	Java Developer Kit 1.8
	C, C#, C++, Visual Basic .NET	Microsoft Visual Studio 2015, 2017
Admin API for Linux	C	GCC
Admin API for Mac OS X	C	Clang, Xcode x.x
Envelope .NET Runtime API	C#	Microsoft Visual Studio 2013, 2015, 2017 Note: Visual Studio 2015.sln should be imported to use in Visual Studio 2013.
Java Envelope Configuration API	Java	Java Envelope Configuration API has been tested with the following compilers: Java Developer Kit 1.8

Current Firmware Version

The table that follows indicates the version of the firmware on Sentinel HL keys that are delivered at the time of the release of Sentinel LDK.

Version of Sentinel LDK	Version of Firmware on...		
	Sentinel HL (Driverless Configuration) Keys	Sentinel HL (HASP Configuration) Keys	(Legacy) Sentinel HASP Keys
7.8, 7.9	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.7.9. 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:

- Mac OS X 10.11
- Android x86

Compilers

Support for Java 9.0.4 has not been tested in Sentinel LDK 7.9.

Sentinel Components

The following Sentinel components are no longer supported and are no longer included on the Sentinel LDK Installation Drive:

- Driver files for Windows XP Embedded
- Sentinel Activation API and samples for Windows, Mac, and Linux

Planned Drop of Support

- Sentinel LDK 7.9 is the last version to support the 32-bit version of Sentinel LDK Envelope for Linux and Sentinel LDK Master Wizard for Linux. These vendor tools will only operate under the 64-bit version of Linux Intel. However, the 64-bit version of Sentinel LDK Envelope will continue to protect applications that run under 32-bit and 64-bit Linux Intel and Linux ARM.
- Sentinel LDK 7.9 is the last version to support protection of 32-bit applications for Mac. Both end user components (Run-time Environment and Vlib) and Vendor Tools (Envelope, Master Wizard) will only be supported for 64-bit.

Sentinel LDK Documentation

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



Most major Sentinel LDK documentation can be found on the Sentinel Customer Community web site, at:

https://sentinelcustomer.gemalto.com/Documentation_Information.aspx

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.
Sentinel LDK Software Protection and Licensing Tutorials	<p>Guide you through the basic procedures of Sentinel LDK to familiarize you with the applications and their functionality.</p> <ul style="list-style-type: none"> • The Demo Kit tutorial is for vendors who wish to evaluate Sentinel LDK. • The Starter Kit tutorial is for vendors who have just 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. 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: <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 EMS Configuration Guide	Provides information on setting up and configuring Sentinel EMS to satisfy the requirements of your organization.
Sentinel 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 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.
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.

Online 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://sentinelcustomer.gemalto.com/Documentation_Information.aspx
- 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%...)
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.

Instructional Videos

A library of instructional videos for Sentinel LDK is available at:
<http://sentinelvideos.gemalto.com/>

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.

Known Issues and Workarounds

The known issues in Sentinel LDK v.7.9 that are likely to have the most significant impact on users are listed below, according to component.

Additional, less-common issues can be found in the Gemalto Knowledgebase at:

https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=aea5eba64f1e720c873b69d18110c713

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>
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> <ol style="list-style-type: none"> 1. When installing Sentinel EMS, the Installer generates the error "Kindly Start the Service -SQLServer(EMSDATABASE) and then click OK". 2. When you click OK, the installation fails with multiple errors. <p>The reason for this is as follows: 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> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <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 more information, 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. </div>
SM-35287	<p>When upgrading from Sentinel LDK v.7.3 through v.7.8 to Sentinel LDK v.7.9, all non-English locales of Customer contacts and Channel Partner contacts in Sentinel EMS are converted to the English locale.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>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> </div> <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 more information, 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 (sent by Sentinel EMS) to display a scheduled report, the report is not displayed when DNS cannot resolve the server hostname present in the link. Instead, the message "This page can't be displayed" is displayed.</p> <p>Workaround: In the <code>etc/host</code> 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 one of the other supported Web browsers, which will allow you to provide text while creating a branded version of the RUS utility.</p>
SM-34794	<p>After searching for an entity (for example: a product) in the Sentinel EMS user interface, the option to sort the list of entities does not work.</p> <p>For entitlements, the issue only occurs if the list extends over more than one page.</p> <p>Workaround (for entitlements): Try to shorten the list to less than one page by specifying a filter value.</p>

End Users, Sentinel LDK Runtime 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 API hasp_update() 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> <ul style="list-style-type: none"> ■ 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>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 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 since 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 has been 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 works in Microsoft Internet Explorer to play local FLV files 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.

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.

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: <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	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: <ul style="list-style-type: none"> ■ For Java 7: Specify <code>java -UseSplitVerifier -jar ProtectedJar.jar</code> ■ For Java 8: Specify <code>java -noverify -jar ProtectedJar.jar</code> If the appropriate flag is not specified, the application may throw java.verifyerror when launched.

Ref	Issue
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:</p> <p>Do the following:</p> <ol style="list-style-type: none"> 1. Use .NET Framework 4.5. 2. Use <pre>CultureInfo.DefaultThreadCurrentCulture = new CultureInfo(...)</pre> instead of <pre>Thread.CurrentThread.CurrentCulture = new CultureInfo(...).</pre>

Ref	Issue
SM-25875	<p>Given the following circumstances:</p> <ol style="list-style-type: none"> A .NET application is protected with Envelope. The protection type includes Windows Shell (with or without Method level). The application attempts to get a module handle using the following method: <pre data-bbox="477 474 1399 590" style="border: 1px dashed red; padding: 5px;"> 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 data-bbox="399 810 1399 1035" style="border: 1px dashed red; padding: 5px;"> [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 like "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-28403	<p>Given the following circumstances:</p> <ul style="list-style-type: none"> ■ A Linux application is protected with Envelope, with protection against debugging. ■ The application calls the wait(&status) system call. This is equivalent to: <code>waitpid(-1, &status, 0)</code> <p>The application may hang.</p> <p>Workaround 1: Call waitpid for a specific child process pid (pid > 0).</p> <p>Workaround 2: Disable the anti-debugging feature in Envelope. Note: This workaround significantly reduces the security of the protected application. Gemalto recommends that you consult with Technical Support before choosing this workaround.</p>
SM-24207	<p>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.</p>

Sentinel LDK Envelope and Data Encryption for Mac OS X

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 a 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.