

Sentinel LDK – v.7.8

Release Notes

Revision History

Part number 007-013811-002, Rev A

Copyrights and Trademarks

© Gemalto 2018. 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.

April 2018 Revision 1804-14

Contents

Sentinel LDK v.7.8 - Release Notes	5
About This Document	5
Product Overview	5
Sentinel Vendor Keys	6
Obtaining Support	6
What's New in Sentinel LDK v.7.8?	7
Sentinel HL Keys Can Be Disabled If Tampering is Detected	7
Run-time Environment Installer for Linux Intel Now Provides Native Support for 64-bit Machines	8
A New Sentinel EMS Web Service Can Fetch Pending License Updates	8
Sentinel EMS Now Supports V2C Package Files	9
Sentinel EMS Is Now Installed with Microsoft SQL Server 2014 SP2 Express	9
Tomcat in Sentinel LDK Has Been Upgraded to Version 8	9
Envelope Can Now Protect Large JAR/WAR Files for Java Applications	10
Sentinel LDK Can Now Ensure the Integrity of .NET Assemblies	10
Android Applications Can Now Be Licensed With a Network Key	10
Enhancements to Envelope for Android Applications	10
Enhancements to Sentinel LDK Envelope for Mac	10
Enhanced Support for Channel Partner Functionality	11
New Clone Protection Scheme for Microsoft Azure Platforms	12
You Can Now Enter a Comment When You Burn a Sentinel HL Key	12
What's Changed in Sentinel LDK v.7.8?	13
Sentinel EMS No Longer Supports Microsoft SQL Server 2008 and SQL Server 2008 R2 Express	13
AutoCAD Sample for Sentinel Licensing API Has Been Moved to Legacy Directory	13
Entitlement COMMITTED Status Has Been Replaced with QUEUED	13
Correction to broadcastsearch Parameter Documentation	13
Email Addresses in Sentinel EMS Can Now Contain Special Characters and Multiple Periods	14
The Legacy Activation API Has Been Updated to Resolve Vulnerabilities	14
Security Updates	14
Reporting a Security Vulnerability	14
Sentinel LDK Vulnerabilities	14
Supported Platforms for Sentinel LDK – End Users and Vendors	15
Supported Platforms for End Users	15
Supported Platforms for Vendors	17
Supported Platforms for Code Samples	20
Tested Compilers for Code Samples	20
Current Firmware Version	21
Dropped Support	22
Platforms for Software Vendors	22

Compilers	22
Sentinel LDK Documentation	22
Documents	22
Getting Started Guides	24
Help Systems - Sentinel LDK and Sentinel EMS User Interfaces	24
Online Help Systems – Sentinel LDK APIs	25
Instructional Videos	26
Software and Documentation Updates	26
Known Issues and Workarounds	27
Sentinel LDK Installation	27
Sentinel EMS	28
End Users, Sentinel LDK Runtime Environment, License Manager, and Customer Tools	29
Sentinel LDK Envelope for Windows Platforms	31
Sentinel LDK Envelope and Data Encryption for Mac OS X	33

Sentinel LDK v.7.8 - Release Notes

About This Document

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



These release notes are subject to change. If you are reading the release notes that were installed with the product, 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.7.8?

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.7.6, 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.

Sentinel HL Keys Can Be Disabled If Tampering is Detected

A native Windows application that is protected with Sentinel LDK Envelope and licensed with a Sentinel HL (Driverless configuration) key can now provide more powerful protection. The Envelope run-time module in the application can disable the key if the module determines that the user has attempted to tamper with the key or with the protected application. Once the key is disabled, the protected application will fail or will display an error message and stop executing, depending on the type of tampering detected.

If the customer's HL key has a Firmware version earlier than 4.54, key disabling is not supported. If tampering is detected, the protected application will fail or will continue to operate, depending on the type of tampering detected. In either case, the customer can continue to use the application afterward.

In Sentinel LDK Envelope, you can enable tamper detection functionality for a protected application by selecting the check box for **Disable key for attempted tampering**. By default, this check box is clear.

The "disabled" state of a key can be viewed at the customer site in Sentinel Admin Control Center or can be determined by the `get_info` function in Sentinel Licensing API.

You have the option to re-enable a disabled HL key using Sentinel EMS or Sentinel License Generation API. For more information, refer to the *Sentinel LDK Software Protection and Licensing Guide*.

If you want to determine the reason that the Sentinel HL key was disabled, you can send a code obtained from a C2V file from the customer to Gemalto Technical Support.

The "disabled" state of an HL key does not affect your ability to send license updates to the key. Any updates that were applied to the key before or after the key was disabled will be in force if you re-enable the key.



Your Master or Developer key must be connected to the machine when you protect an application with the tamper detection functionality. This functionality is not supported for the DEMOMA Batch Code.

Run-time Environment Installer for Linux Intel Now Provides Native Support for 64-bit Machines

The Sentinel Run-time Environment for Linux Intel machines now provides native support for both 32-bit and 64-bit machines. As a result:

- You are no longer required to provide 32-bit support libraries (x86 compatibility packages) for 64-bit architectures. (The script for 32-bit compatibility packages is no longer provided.)



To support your application on both 32-bit and 64-bit architectures, you should be sure to provide both 32-bit and 64-bit customized Vendor libraries with the Run-time Environment installer.

- Native 64-bit versions of the aksusbd and hasplmd daemons are provided.
- The `/usr/sbin/winehasp` daemon is not required in order to support Wine applications and is no longer installed. Wine applications can be supported directly using Runtimeless APIs.

A New Sentinel EMS Web Service Can Fetch Pending License Updates

When called from a protected application, the **Fetch Pending Updates (V2C) Using C2V** web service accepts as input a C2V file from the customer's machine and returns a single V2CP (vendor-to-customer package) file. This file contains all pending V2C license updates (if any) from Sentinel EMS for the protection key. When the V2CP file is applied, it will automatically apply all pending update in sequence to the protection key.

This new web service simplifies license updates. The web service makes it possible to automate the update process and removes the need for the user to send C2V files and apply V2C files. This significantly simplifies the process of keeping protection keys in sync with Sentinel EMS.

You can set up your protected application to call this web service periodically at an interval determined by a parameter in Sentinel EMS Admin Console. In Admin Console, you specify a value for the parameter **Client Polling Frequency**. When a protected application calls the **Fetch Pending Updates Using C2V** web service, Sentinel EMS returns the polling frequency specified in the Admin Console as an added header in each successful response to the web service call.

You can use this value programatically in the protected application as a time interval to call the **Fetch Pending Updates Using C2V** web service periodically. In this manner, you can control the polling frequency for all your applications from a single point and you can alter the polling frequency dynamically for all protected applications that call this web service.

The Sentinel Activation API sample code file demonstrates a method that can be used to read the polling frequency value from the web service response.

For more information refer to the *Sentinel EMS Web Services Guide*.

Sentinel EMS Now Supports V2C Package Files

When Sentinel EMS generates V2C (vendor-to-customer) transactions, it can now optionally combine multiple V2C transactions into a single file, known as a V2CP (vendor-to-customer package) file..

A V2CP file contains both the latest V2C license update and any previous updates (V2C files) which the end user may not have applied. This simplifies license updates and ensures that updates can always be applied, regardless of whether or not the end user applied previous updates.

When the V2CP file is processed by the License Manager on the end user's machine, the file is broken down into its component V2C files. Each V2C file is examined to determine if it has been applied previously to the protection key. V2C files that were applied previously are discarded. V2C files that were not applied previously are now applied in the correct sequence.

In the current release of Sentinel EMS, V2CP files are only generated in the following circumstances:

- The **Fetch Pending Updates (V2C) Using C2V** web service (described earlier) is called.
- Sentinel EMS Web interface is used to generate a transaction to re-enable an HL key that was disabled due to tampering activity.

(In the next release of Sentinel EMS, V2CP files will be available in all situations where Sentinel EMS Web Services or Web interface issues V2C transactions.)

Unlike V2C files, a V2CP file does not contain any cleartext (readable) information. However, once the V2CP file has been applied on the end user's machine, the individual V2C files that the V2CP file contained are accessible in the relevant **installed** directory and can be viewed as in the past.

Sentinel EMS Is Now Installed with Microsoft SQL Server 2014 SP2 Express

Sentinel EMS now supports SQL Server 2014 Express. Sentinel EMS no longer supports SQL Server 2008 or SQL Server 2008 R2 Express.

If you use the **Express** setup type to install Sentinel EMS:

- For a new installation of Sentinel LDK, the Sentinel LDK Installation Wizard now installs SQL Server 2014 Express.
- For an upgrade of Sentinel LDK, if you currently have SQL Server 2008 R2 Express installed on the local machine, the Sentinel LDK Installation Wizard upgrades SQL Server to SQL Server 2014 Express.

If you use the **Advanced** setup type to upgrade Sentinel EMS from an earlier version, Sentinel LDK Installation Wizard does not allow you to connect to an existing installation of SQL Server 2008 or SQL Server 2008 R2 Express.

For the full list of supported versions of SQL Server, see "[Sentinel EMS Database](#)" on page 18.

Tomcat in Sentinel LDK Has Been Upgraded to Version 8

When installing or upgrading Sentinel EMS, the Sentinel LDK installation wizard now installs Tomcat version 8.5.23 instead of version 7. The newer version of Tomcat contains significant changes, resulting in improved security, stability and performance.

Envelope Can Now Protect Large JAR/WAR Files for Java Applications

Sentinel LDK Envelope can now be used to protect Java applications that are up to 15 MB in size and that contain a very large number of classes and methods.

Sentinel LDK Can Now Ensure the Integrity of .NET Assemblies

Sentinel LDK Envelope now ensures the integrity of .NET assemblies both when protecting the assemblies and when the protection application is executed:

- When protecting an assembly, Envelope ensures that the assembly is signed. It is not necessary to re-sign the assembly after it has been protected.
- During execution of the protected application, the Envelope run-time module detect any changes to the assembly including modifications in the metadata or signing by an unauthorized body

Android Applications Can Now Be Licensed With a Network Key

A protected Android application can be licensed by any remote protection key that supports concurrency. The remote protection key must be located on Windows or Linux Intel machine on which Sentinel Run-time Environment has been installed.

This feature has been tested with protection keys located in the same LAN as the Android platform. Detaching of a license to an Android platform is not supported.

For APK or native binaries that are protected with Sentinel LDK Envelope, concurrency is only supported when you define a custom login scope to locate the relevant License Manager or protection key. For more information, see the Advanced Protection parameters in the Sentinel LDK Envelope help system.

Enhancements to Envelope for Android Applications

- Sentinel LDK Envelope now supports Android 7 applications.
- Sentinel HL keys are now supported with Android native binaries.
- Sentinel LDK Envelope now supports applications that have more than one launch activities.

Enhancements to Sentinel LDK Envelope for Mac

Sentinel LDK Envelope now provides a new protection engine to improve support of Mac executables and dynamic libraries built with Xcode 6 and later.

To build Mach-O binaries, ensure that the deployment target in your Xcode project file is set to 10.9 or later. Deployment target 10.8 is also compatible in certain cases. (It may be necessary to install a newer version of Xcode on your machine to satisfy these requirement.)

Binaries that are built with deployment target 10.7 or earlier, built with macOS SDK 10.8 or earlier, or built with certain other development tools continue to be supported with a legacy protection engine.

You can configure Envelope to indicate which protection engine to use. By default, Envelope uses the new protection engine. Gemalto recommends that you first try the current protection engine to protect your application. If Envelope rejects older binaries or displays warning messages for them, you can switch to the legacy protection engine by selecting the **Use legacy engine** option in the Settings screen.

Note that the legacy protection engine will be discontinued in one of the next releases of Sentinel LDK.

Enhanced Support for Channel Partner Functionality

(This enhancement was included in the Sentinel LDK v.7.7 update.)

Support for channel partner functionality has been significantly enhanced in Sentinel EMS.

You can now associate a channel partner with specific Products in the catalog. When you create an entitlement for a given channel partner customer, only associated Products will be available for the entitlement.

A new user type called **Channel Partner** now exists in Sentinel EMS. When you define a new user for Sentinel EMS, you can designate the user as a **Channel Partner** user and associate the user with a channel partner.

A Channel Partner user will be able to perform the following functions in Sentinel EMS:

- Create and manage their own end-user customers.
- View, produce, and activate entitlements for their customers.
- Resend e-mails for entitlements for their customers.
- Display product keys for entitlements for their customers.
- Check in, browse, and view details of C2V files for their customers.

All other Sentinel EMS functionality will be blocked for these users. When a Channel Partner user logs in to Sentinel EMS, the landing page will be the Entitlements page.

To use the enhanced functionality described above, you must purchase the new **Channel Partner** module for your Master key.

Note the following limitations:

- The enhanced Channel Partner functionality is currently not supported by Sentinel EMS Web Services.
- The enhanced Channel Partner functionality is not supported by Web browsers that support Java applets.
- Existing Sentinel LDK vendors (a vendor who has introduced a Master key) who want to evaluate the new Channel Partner functionality must request a 30-day evaluation license (948-000112-001) from their Gemalto representative, even when working with the DEMOMA Batch Code. Evaluators (vendors who have not yet introduced a Master key) can evaluate Channel Partner functionality without a special evaluation license.
- Sentinel LDK provides a tool for migrating from the legacy Business Studio product to Sentinel EMS. However, this tool does not migrate the Channel Partner data and

functionality that existed in Business Studio to Sentinel EMS. For more information see *Migration Guide: Sentinel HASP to Sentinel LDK*.



Before working with the new Channel Partner functionality, it may be necessary to resolve conflicts that arise when a customer is associated with multiple channel partners. For more information, see "Modifying the Sentinel EMS Database for Advanced Channel Partner Functionality" in the *Sentinel LDK Installation Guide*.

New Clone Protection Scheme for Microsoft Azure Platforms

(This enhancement was included in the Sentinel LDK v.7.7 update.)

The **VMType3** clone protection scheme is designed to provide strong and reliable clone protection for the Microsoft Azure virtualization platform. This scheme addresses the following situations:

- The scheme ensures that a protected application in a server virtualized environment cannot be used if the license is copied from one virtual machine to another.
- The scheme ensures that an SL UserMode licenses is protected against misuse by UserMode secure storage wipeout.
- With other clone protection schemes, performing Start-Stop-Restart of the Azure infrastructure causes the platform to be reported as Cloned. This does not occur with the **VMType3** clone protection scheme.

The following restrictions apply:

- The **VMType3** clone protection scheme is not supported for the SL UserMode enforcement type for Linux platforms.
- Sentinel LDK Run-time Environment version 7.61 or later must be available to the protected application.

You Can Now Enter a Comment When You Burn a Sentinel HL Key

(This enhancement was included in the Sentinel LDK v.7.7 update.)

Sentinel EMS now enables you to enter a comment in the Produce Sentinel HL Keys screen for each Sentinel HL key to be burned. The comments are stored in the Sentinel EMS database.

When you view generated HL keys in the Previous Activations screen, the comment that you entered for each key is displayed along with other information relating to the key.

What's Changed in Sentinel LDK v.7.8?

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

Sentinel EMS No Longer Supports Microsoft SQL Server 2008 and SQL Server 2008 R2 Express

Sentinel EMS now supports SQL Server 2014 Express. Sentinel EMS no longer supports SQL Server 2008 or SQL Server 2008 R2 Express.

If you use the **Express** setup type to install Sentinel EMS:

- For an upgrade of Sentinel LDK, if you currently have SQL Server 2008 R2 Express installed on the local machine, the Sentinel LDK Installation Wizard upgrades SQL Server to SQL Server 2014 Express.

If you use the **Advanced** setup type to upgrade Sentinel EMS from an earlier version, Sentinel LDK Installation Wizard does not allow you to connect to an existing installation of SQL Server 2008 or SQL Server 2008 R2 Express.

For the full list of supported versions of SQL Server, see "[Sentinel EMS Database](#)" on page 18.

AutoCAD Sample for Sentinel Licensing API Has Been Moved to Legacy Directory

The sample that demonstrates the use of Sentinel Licensing API when working in the AutoCAD environment has been moved in the Sentinel LDK `%ProgramFiles(x86)%\Gemalto Sentinel\Sentinel LDK\` directory structure:

from: `\Samples\Runtime\AutoCAD\`

to: `\Legacy\Samples\Runtime\AutoCAD\`

Entitlement COMMITTED Status Has Been Replaced with QUEUED

The COMMITTED status for entitlements in Sentinel EMS Web Services is deprecated and has been replaced by the QUEUED status. The related action of COMMIT has been replaced with QUEUE.

Correction to broadcastsearch Parameter Documentation



This change was included in the Sentinel LDK v.7.7 update.

The documentation of the possible values for the **broadcastsearch** parameter in the *Sentinel LDK Software Protection and Licensing Guide* contained an error and has been corrected. The corrected possible values for this parameter are:

- 0 — Disable broadcasts.
- 1 — Enable broadcasts. Default.

Email Addresses in Sentinel EMS Can Now Contain Special Characters and Multiple Periods



This change was included in the Sentinel LDK v.7.7 update.

The routine used to validate email addresses in Sentinel EMS now accepts special characters (=%#\$~) as part of the address. In addition, email addresses can now contain multiple periods in the domain segment of the address.

The Legacy Activation API Has Been Updated to Resolve Vulnerabilities

The DLL files provided for the legacy Activation API update package have been updated to resolve OpenSSL vulnerabilities. The latest OpenSSL library (v1.0.2n) was used to rebuild **hasp_act_windows.dll** and **hasp_act_windows_x64.dll** version 2.52.

Security Updates

This section describes security issues that may affect Sentinel products and that have been resolved in Sentinel Run-time Environment v.7.80 or later.

For the latest information regarding these issues or 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 then please send it to Gemalto using the links provided on the Web page provided above.

Sentinel LDK Vulnerabilities

The vulnerabilities listed below affect the License Manager service of HASP SRM, Sentinel HASP and Sentinel LDK products. These vulnerabilities are resolved in Sentinel Run-time Environment version 7.80.

- (SM-26010) A cross-site scripting (XSS) vulnerability in the Admin Control Center logs has been resolved.

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 7.80
Mac	Version 7.80
Linux Intel	Version 7.80



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.

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 10 Version 1709 <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> Windows 10 Insider Preview builds are not supported. </div> <p>The latest service packs and security updates must be installed.</p>
Windows Embedded	<ul style="list-style-type: none"> ■ (x86 only) Windows 7 SP1 Embedded standard

System	Supported Versions	
Mac	<ul style="list-style-type: none"> ■ Mac OS X 10.11 ■ macOS 10.12 ■ macOS 10.13 (High Sierra) <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>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 29.</p> </div>	
Linux	Linux Intel (x86 and x86_64)	<ul style="list-style-type: none"> ■ OpenSUSE Leap 42.3 ■ Red Hat EL 6.9, 7.4 ■ Ubuntu Server 14.04, 16.04 ■ Ubuntu Desktop 16.04 ■ Debian 9 ■ CentOS 7.4 <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	<p>Sentinel LDK Run-time Environment was tested on Linux platforms with Wine 1.7.28.</p>
Android	Android ARM (32-bit) Android x86 (32-bit)	<p>Android 5.1.1, 6.x, 7.x</p>
	Android Architecture	<p>The following architecture is supported:</p> <ul style="list-style-type: none"> ■ armv7 ■ armv7a ■ x86
	Android ABI	<p>Sentinel LDK Envelope supports Android applications designed for the following Android application binary interfaces:</p> <ul style="list-style-type: none"> ■ armeabi ■ armeabi-v7a ■ x86

System	Supported Versions
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 13 for Mac ■ VMware Player 6.0.3 ■ VMware Workstation 14 ■ VMware ESXi 5.5, 6.0 ■ Hyper-V Server 2016 (SL only) ■ Xen 4.6 ■ KVM (RHEL 7.4, Ubuntu 16.04 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>

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 version 41 or later
- Mozilla Firefox version 58 or later
- Google Chrome version 63 or later
- Safari version 11 or later

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 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> <ul style="list-style-type: none"> ■ 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> <ul style="list-style-type: none"> ■ Microsoft SQL Server 2016

Web Browsers for Sentinel EMS

- Microsoft Internet Explorer version 11
- Mozilla Firefox version 58 or later
- 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 28.

- Google Chrome version 63 or later





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"> ■ See supported Windows platforms for Sentinel LDK Run-time Environment (above). <p>Requires screen resolution 1280 by 1024 pixels with 24-bit color quality</p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">  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;">  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>
Mac	<ul style="list-style-type: none"> ■ macOS 10.12 ■ macOS 10.13.2 (High Sierra) <p>Applications built on the Cocoa framework are supported.</p>
Linux Intel	<ul style="list-style-type: none"> ■ OpenSUSE Leap 42.3 ■ Red Hat EL 7.4 (x86 and x86_64) ■ Ubuntu Server 16.04 (x86 and x86_64) ■ Ubuntu Desktop 16.04 (x86 and x86_64) ■ Debian 9.x (x86 and x86_64) ■ CentOS 7.4 (x86 and x86_64) <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 and x86 platforms (MIPS platform is not supported.)
Java	Java 9.0.4

Supported Platforms for Code Samples

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

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, 9.0.4
Licensing API for Mac OS X	Java	Java Developer Kit 1.8, 9.0.4
	C	GCC, Xcode
Licensing API for Linux	Java	Java Developer Kit 1.8, 9.0.4
	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, 9.0.4
Activation API for Windows	C	Microsoft Visual Studio 2013, 2015, 2017 You may need to covert the provided workspace for the VS version used.
	Java	Java Developer Kit 1.8, 9.0.4
Activation API for Mac OS X	Java	Java Developer Kit 1.8, 9.0.4
Activation API for Linux	Java	Java Developer Kit 1.8, 9.0.4

API	Programming Language	Tested Compilers
Runtime Environment Installer	C	Microsoft Visual Studio 2013, 2015, 2017
	MSI	InstallShield 12 InstallShield 2013
Admin API for Windows	Java	Java Developer Kit 1.8, 9.0.4
	C, C#, C++, Visual Basic .NET	Microsoft Visual Studio 2015, 2017
Admin API for Linux	C	GCC
Admin API for Mac OS X	C	GCC, Xcode
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, 9.0.4

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	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.7.8. 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

Sentinel LDK can no longer be installed on the following platforms:

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 2003 Server
- Microsoft Windows 2008 Server

Sentinel EMS is no longer compatible with Microsoft SQL Server 2008 or SQL Server 2008 Express.

Compilers

Support for the following compilers has been discontinued:

- Java Developer Kit 1.7
- Microsoft Visual Studio 2010
- Delphi 2007
- Wise for Windows Installer 7.1
- InstallShield 2012 Spring

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.
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

Document	Description
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.)

Sentinel LDK API	Description
Licensing API Reference (formerly Run-time API)	Provides the developer with an interface to use the licensing and protection functionality available in the Sentinel LDK Run-time Environment.
Run-time 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.7.8 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>
LDK-12131	<p>When the schedule for checking for updates in Sentinel LDK Software Manager is set to "Manual", the setting is not saved. Instead, Software Manager reverts to the default setting (every 3rd Wednesday at 15:00).</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;"> <ul style="list-style-type: none">  <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>

Sentinel EMS

Ref	Issue
EMSLDK-5168	<p>When packaging a Run-time Environment installer with a V2C file for one or more Products in Sentinel EMS, you cannot include a Product that only has the locking type SL UserMode. An attempt to install such a package will fail with the message "V2C unknown HASP API 49 Error". Sentinel EMS does not currently prevent you from creating such a package.</p> <p>Workaround: When generating the RTE installer in Sentinel EMS, use the locking type SL-AdminMode for Products.</p>
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 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, 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>

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 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, 8, or 9 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, 9: 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 style="margin-left: 40px;">CultureInfo.DefaultThreadCurrentCulture = new CultureInfo(...)</pre> instead of <pre style="margin-left: 40px;">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 1037" 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>

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.