

Sentinel[®]LDK

Sentinel LDK v.7.0
Release Notes



Document Revision History

Part number 007-012273-001, Rev B

Build 1310-1

Disclaimer and Copyrights

Copyright © 2013, SafeNet, Inc. All rights reserved. <http://www.safenet-inc.com/>

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them 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. SafeNet, Inc. 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.

SafeNet[®] and Sentinel[®] are registered trademarks of SafeNet, Inc. All other product names referenced herein are trademarks or registered trademarks of their respective manufacturers.

Confidential Information

Sentinel LDK is designed to protect your applications from unauthorized use. The less information that unauthorized people have regarding your security system, the greater your protection. It is in your best interest to protect the information herein from access by unauthorized individuals .

Contents

About This Document	5
Product Overview	5
Sentinel Vendor Keys	6
Obtaining Support	6
Help Us to Improve Sentinel LDK	6
What's New in This Release?	7
Changes to the Original Release of Sentinel LDK v.7.0	7
New "AppOnChip" Feature in Sentinel LDK Envelope	8
Sentinel HL Network Keys Can Now Be Upgraded to Driverless Configuration	8
Enhanced Security for SL-UserMode Licenses	9
License Manager Can Now be Easily Replaced in Runtimeless Installations	10
Support for Mac OS X 10.8.5	10
Additional Enhancements to Sentinel LDK Envelope	11
Enhanced Usability in the Sentinel EMS User Interface	11
Enhancements to the Sentinel Licensing API	11
Enhancements to the Sentinel License Manager and Admin Control Center	11
Enhancements to Clone Protection	12
Added Support for SL Legacy licenses	12
Enhancements to the Sentinel LDK Master Wizard	12
Easier Access to Working Online in Vendor Tools	13
Support for Windows CE	13
What's Changed in This Release?	13
Changes to Admin Control Center	13
Name of License Manager Service	13
Supported Platforms for Sentinel LDK – End Users and Vendors	14
Supported Platforms for End Users	14
Supported Platforms for Vendors	15
Supported Versions for Windows CE	18
Dropped Support	18
Platforms for End Users	19
Sentinel LDK Documentation	20
Documents	20
Help Systems - User Interfaces	21
Online Help Systems – Sentinel LDK APIs	22
Software and Documentation Updates	23
Known Issues and Workarounds	24
Sentinel Vendor Suite Installation	24
Sentinel EMS	24
Sentinel LDK Master Wizard	25
Sentinel LDK Runtime Environment Installer	26

Sentinel LDK Runtime Environment and Customer Tools26

Sentinel LDK ToolBox 27

Sentinel LDK Envelope for Windows Platforms 27

Sentinel LDK Envelope and Data Encryption for Mac OS X 31

Sentinel LDK Envelope and Support for ARC in Mac OS X 33

Sentinel LDK v.7.0 - 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, SafeNet 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.safenet-inc.com/API_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, provisional (trial/grace), 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:
<http://www.safenet-inc.com/contact-us/>
- **Technical Support** - To obtain assistance in using SafeNet products, feel free to contact our Technical Support team:
 - Phone: 800-545-6608 (US toll free), +1-410-931-7520 (International)
 - E-mail: support@safenet-inc.com
 - URL: <http://sentinelcustomer.safenet-inc.com/sentinelsupport/>
- **Downloads** - You can download installers and other updated components using this URL:
www.sentinelcustomer.safenet-inc.com/sentineldownloads/

Help Us to Improve Sentinel LDK

You can make a difference! We invite you to send us your ideas and opinions, and tell us what you like (and don't like) about Sentinel LDK. Your input can help shape future versions of the product.

Feedback on Sentinel LDK can be sent to: ldkfeedback@safenet-inc.com

What's New in This Release?

This section describes the main features and enhancements that are introduced in Sentinel LDK v.7.0.

Changes to the Original Release of Sentinel LDK v.7.0

A number of important changes have been made to the original release of Sentinel LDK 7.0. The following additional versions of Sentinel LDK have been released:

Sentinel LDK v.7.0.2.

The changes in Sentinel LDK v.7.0.2 are as follows:

- Support for Mac OS X has been restored. The original release did not support Mac.
- Windows 8.1 is supported instead of Windows 8.
- Problems with migration from Business Studio Server ("BSS") to Sentinel EMS have been resolved:
 - A problem with Master key detection in BSS would occur when the vendor migrated from BSS to Sentinel EMS on the same machine.
 - A communication error with BSS would occur during the migration process.

Sentinel LDK v.7.0.3.

This release includes all the corrections provided in Sentinel LDK v.7.0.2. In addition, this release resolves a problem with the handling of file names in Sentinel LDK Envelope for Mac.

What should I install?

Last version of Sentinel LDK installed	Distributor of Windows applications	Distributor of Linux applications	Distributor of Mac applications
Original v.7.0 release	Proceed to install Sentinel LDK v.7.0.3. Follow the upgrade path ("Upgrading From Sentinel LDK v.6.x") in the <i>Sentinel LDK Installation Guide</i> .		
v.7.0.2	No action required.	No action required.	Re-install Sentinel LDK v.7.0.3 Envelope for Mac.

The documentation and help systems in this release are the same as those provided in Sentinel LDK v.7.0. They continue to be identified as Sentinel LDK v.7.0.

New "AppOnChip" Feature in Sentinel LDK Envelope

Sentinel LDK Envelope now incorporate the "AppOnChip" feature for applications that are protected using Sentinel HL (Driverless configuration) keys. Envelope extracts selected code from the protected binary of an application and converts the code so that it is executed by the Sentinel HL key during application runtime. This creates a strong binding between the protected application and the presence of the protection key, making reverse engineering of the protected code virtually impossible.

Sentinel LDK Envelope automatically generates a table of functions in the protected application that are eligible to be protected with AppOnChip. In the Envelope user interface, you can review the list of eligible functions, and select the functions to be protected with AppOnChip.



Your Developer key must be connected to the machine where Envelope is running when you protect an application with AppOnChip.

In the current release, the following limitations apply for the application to protect:

- Windows 32-bit applications only
- EXE files only (no DLL support)
- Native x86 binaries only (.NET assemblies are not supported)

In the current release, AppOnChip is available to all vendors as part of the basic Sentinel LDK license. In future releases, the use of AppOnChip will, in some cases, require the purchase of a separate license module.

Sentinel HL Network Keys Can Now Be Upgraded to Driverless Configuration

Sentinel HL (HASP configuration) Net keys and NetTime keys that were previously delivered to customers can now be upgraded to Sentinel HL (Driverless configuration) keys in the field. In Driverless configuration, these keys will employ HID drivers instead of HASP key drivers. (HID drivers are an integral part of the operating system.) As a result, these keys are less subject to issues related to operating system upgrades.



An application that is protected with version 6.3 or 6.4 of Sentinel LDK, Licensing API libraries and/or Envelope will work correctly after the Sentinel HL (HASP configuration) key that licenses the application is upgraded to the Driverless configuration. However, the requirement for the Run-time Environment will not change.

The tables that follow summarize the requirements for working with HL keys.

Standalone HL Keys

Version of Licensing API or Envelope used to protect the application (lower of the 2)	HASP HL key or Sentinel HL (HASP configuration) key	Sentinel HL (Driverless configuration) key
HASP SRM, Sentinel HASP, or Sentinel LDK v.6.0 or v.6.1	Requires Run-time Environment from same (or later) version that was used to protect the application	Not supported. See the warning below.
Sentinel LDK v.6.3	Requires Run-time Environment from Sentinel LDK v.6.3 or later	
Sentinel LDK v.6.4	Requires Run-time Environment from Sentinel LDK v.6.4 or later	
Sentinel LDK v.7.0	Requires Run-time Environment from Sentinel LDK v.7.0 or later	Under Windows, use of Run-time Environment from Sentinel LDK v.7.0 or later is optional.

Net and NetTime HL Keys

Version of Licensing API or Envelope used to protect the application (lower of the 2)	HASP HL key or Sentinel HL (HASP configuration) key	Sentinel HL (Driverless configuration) key
HASP SRM, Sentinel HASP, or Sentinel LDK v.6.0 or v.6.1	On the machine where the HL key is connected: Requires Run-time Environment from same (or later) version that was used to protect the application	Not supported. See the warning below.
Sentinel LDK v.6.3	On the machine where the HL key is connected: Requires Run-time Environment from Sentinel LDK v.6.3 or later	
Sentinel LDK v.6.4	On the machine where the HL key is connected: Requires Run-time Environment from Sentinel LDK v.6.4 or later	
Sentinel LDK v.7.0	On the machine where the HL key is connected: Requires Run-time Environment from Sentinel LDK v.7.0 or later	

Warning: An application that is protected with version 6.1 or earlier of Sentinel LDK libraries, Licensing API libraries and/or Envelope will stop working if the Sentinel HL (HASP configuration) key that licenses the application is upgraded to the Driverless configuration.

The upgrade process for the Sentinel HL key is not reversible.

Enhanced Security for SL-UserMode Licenses

In the past, SL-UserMode licenses provided a relatively low level of security for licenses of the type: executions, time period, provisional, and re-host. Security for these type of licenses has been significantly improved in the current release of Sentinel LDK.

The C2V file used to generate or update the SL-UserMode license must be created using RUS (**hasprus.exe** tool) or Licensing API from Sentinel LDK 7.0 or later. C2V files created using older version of Sentinel LDK are not compatible with the enhanced SL-UserMode license security. In the event that you must work with a C2V file that was created using an earlier version of Sentinel LDK, you can prevent a compatibility error by using the tag `<enforce_secure_storage_id>` in License Generation API or by setting the global parameter **Enforce SL-UserMode format v2.0** in Sentinel EMS Admin Console.

License Generation API allows you to handle the compatibility issue for individual C2V files.



However, once you enable **Enforce SL-UserMode Format v2.0**, Sentinel EMS will only accept new C2V formats. If you disable this parameter, Sentinel EMS will accept old C2V files and generate less secure V2C files even when the C2V files are created using the new (LDK 7.0) format.

License Manager Can Now be Easily Replaced in Runtimeless Installations

The Integrated (Embedded) License Manager is used in situations where the Sentinel Run-time Environment cannot be used (for example, due to limited user permissions). This License Manager is available under Windows and is used to access the following protection keys:

- local Sentinel HL (Driverless configuration) keys
- remote keys (Note: The RTE must be present on the remote machine where the key is connected)
- SL UserMode keys.

To upgrade this License Manager until now, it was necessary to re-compile protected applications that employ the Licensing API or re-protect applications that employ Sentinel LDK Envelope.

For applications that are protected using the Licensing API provided with LDK 7.0 or that are protected using the Sentinel LDK Envelope, you can upgrade from the Integrated License Manager to the new External License Manager by simply adding the file **hasp_rt.exe** in the directory that contains the protected application. You can upgrade the License Manager in future versions by simply replacing this file with a new version.

Support for Mac OS X 10.8.5

Sentinel LDK now supports Mac OS X 10.8.5. Applications for Mac that are protected using Sentinel LDK Envelope for Mac can now be code signed. Signing is mandatory to satisfy the requirements that Apple introduced to distribute trusted applications.



You should only sign an application after it has been protected with Envelope. Protection of a signed application with Envelope removes the signature. (A relevant message is added to the Envelope log file.) message. Protection of signed applications is not recommended.

Additional Enhancements to Sentinel LDK Envelope

Sentinel LDK Envelope and Sentinel LDK Data Encryption Utility have been enhanced as follows:

- Sentinel LDK Envelope can now protect multiple JAR files in a single directory for a Java application.
- By default, Envelope protects the import of an application or DLL for Windows applications. You now have the ability to exclude specific libraries from import protection. This is an alternative to disabling import protection entirely (using the advanced property `IMPORT_PROTECTION`).
- Sentinel LDK Envelope can now protect methods that get parameters by REF.
- In addition to mixed-mode EXEs, Envelope now supports protection of mixed-mode DLLs. Note that certain protection parameters (such as string encryption, obfuscate symbols, apply compression) will not be applicable in this case.

Enhanced Usability in the Sentinel EMS User Interface

The design and usability of the Sentinel EMS user interface has been significantly improved. The user interface now provides a more intuitive, consistent, and reliable work environment, making the interface easier and more comfortable to work with.

Enhancements to the Sentinel Licensing API

The Sentinel Licensing API has been enhanced as follows:

- You can now consume multiple seats in a single API call. This is accomplished by specifying the tag `<feature network_seats_to_consume="value"/>` in the XML login scope. In Sentinel Admin Control Center, the seats consumed are displayed in a single Session entry rather than in multiple Session entries. The seats are returned to the pool upon logout.

Enhancements to the Sentinel License Manager and Admin Control Center

The Sentinel License Manager and Admin Control Center have been enhanced as follows:

- Admin Control Center and the License Manager can now be protected against all access from outside the local machine, including remote Admin Control Centers, APIs, and foreign tools. This is achieved by listening on local sockets only. For more information, see the new Network tab in the Admin Control Center Configuration page.
- Admin Control Center now uses server-side HTTP basic authentication when the user chooses the option to use password protection for the Admin Control Center configuration pages.
- In Sentinel EMS, you can now prevent the License Manager from formatting a Sentinel protection key from which a Product is currently detached. In Sentinel License Generation API, a new tag `<check_detached_license_before_format_key>` can be specified in the license definition when formatting or clearing a protection key to ensure that no Products are currently detached.

Enhancements to Clone Protection

- Sentinel LDK now allows you to enable or disable protection against running multiple instances of a protected application on multiple cloned or virtual machines. (Previously, this protection was always enabled.)
- Clone protection can now be disabled at the Product level for Sentinel SL keys. You can allow trusted end users to activate SL licenses on virtual machines and still be able to move them to different physical hosts. (This option reduces the level of protection and should only be used if needed as a workaround.)

Added Support for SL Legacy licenses

Sentinel LDK now provides added flexibility to support SL Legacy licenses, created by Sentinel HASP Business Studio.

- You can now set a global parameter in Sentinel EMS that prevents automatic upgrade of SL-Legacy licenses to SL-AdminMode licenses when you create an update to an existing SL-Legacy license.
- You can include a new tag (`<enable_sl_legacy_support>`) in template files for Sentinel License Generation API to prevent automatic upgrade of SL-Legacy licenses to SL-AdminMode licenses when you create an update to an existing SL-Legacy license.

By preventing the upgrade of SL-Legacy licenses, you enable existing customers to continue working with the older Run-time Environment that is currently installed on their computers.

Note that the following new functionalities that are supported for SL-AdminMode licenses are not available for SL-Legacy licenses:

- Rehost a license to a different computer
- Readable license certificates
- Disallow formatting of a protection key when a Product is currently detached

If any of this functionality is included in the license update, the license is upgraded to SL-AdminMode regardless of the setting specified for the `<enable_sl_legacy_support>` tag.

Enhancements to the Sentinel LDK Master Wizard

The Sentinel LDK Master Wizard has been enhanced as follows:

- In the past, it may have been necessary for the vendor to work with a "HASP" Master or Developer key and a "Sentinel LDK" Master or Developer key in parallel when dealing with Sentinel HL (Driverless configuration) keys. The Sentinel LDK Master Wizard has been enhanced so that the HASP Master key and HASP Developer key will be automatically upgraded to support working with Sentinel HL (Driverless configuration) keys when they are re-introduced. As a result, you can work with just the HASP Vendor keys. You are no longer required to connect the HASP Vendor keys and Sentinel Vendor keys in parallel.

(This enhancement was delivered as a software update to vendors who are working with Sentinel LDK 6.4.)

Easier Access to Working Online in Vendor Tools

Sentinel LDK Envelope and Sentinel LDK ToolBox now contain a message at the bottom of the screen when you are not connected to the Sentinel EMS Server.

There are several benefits when you connect to the server (see the message text for more information). You can click a link in the message to easily log in to the server. You can also close or suppress the message.

Support for Windows CE

The Sentinel LDK Run-time Environment (version 5.95) and Envelope deliverables are now supported for Windows CE versions 5.0 and 6.0.

What's Changed in This Release?

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

Changes to Admin Control Center

Newer versions of Windows do not allow the use of Internet Explorer proxy configuration settings to download Admin Control Center Language Pack files. If you are using a proxy server, specify proxy configuration settings in Admin Control Center on the new **Network** tab of the Configuration page.

Name of License Manager Service

The name of the License Manager service that is included in the Sentinel LDK Run-time Environment has been changed from **Sentinel Local License Manager** to **Sentinel LDK License Manager**. This name is displayed in the Services window for the Windows operating system.

Supported Platforms for Sentinel LDK - End Users and Vendors

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 6.60 Sentinel LDK Run-time Environment has been certified by Microsoft as "Compatible with Windows 8" (x86 and x64).
Mac	Version 7.0
Linux	Version 2.2.1



To support all the latest enhancements in Sentinel LDK 7.0, 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"> ■ (x86 and x64) Windows XP, Windows Vista, Windows 7, Windows 8.1, Windows Server 2003, Windows 2008, Windows 2008 R2, Windows Server 2012 ■ The latest service packs and security updates must be installed. ■ (x86 only) Windows XP Embedded standard ■ (x86 only) Windows 7 Embedded standard
Mac	<ul style="list-style-type: none"> ■ Mac OS X 10.6.8 (32-bit and 64-bit) ■ Mac OS X 10.7.5 ■ Mac OS X 10.8.5
Linux	<ul style="list-style-type: none"> ■ OpenSUSE 12.3 (x86 and x86_64) ■ Red Hat EL 5.9, 6.4 (x86 and x86_64) ■ Ubuntu Server 10.04 (x86 and x86_64) ■ Ubuntu Desktop and Server 12.04 (x86 and x86_64) ■ Debian 6.0.x (x86 and x86_64) ■ CentOS 6.4 (x86 and x86_64) <p>The latest service packs and security updates must be installed.</p>

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"> ■ Virtual Box 4.2.12 ■ Parallel Desktop 8 for Mac ■ VMware Player 5.0.2 ■ Hyper-V Server 2012 (SL only) ■ VMware Workstation 9.0.2 ■ VMware ESXi 4.x (Note: This has been tested with Windows XP and Windows 7 Guest operating systems only.) ■ VMware ESXi 5.1 ■ XEN 4.2.1 ■ KVM (RHEL 6, Ubuntu 12.04 server, Debian)
Wine	Sentinel LDK Run-time Environment was tested on Linux platforms with Wine 1.4.1.

Web Browsers for Sentinel Admin Control Center


- Microsoft Internet Explorer (32-bit) versions 8, 9, 10
- Mozilla Firefox (32-bit) version 22
- Google Chrome (32-bit) version 23 or later
- (Mac) Safari 5.0, 6.0

Supported Platforms for Vendors

Sentinel EMS Service

System	Supported Versions
Windows	(x86 and x64) Windows XP, Windows Server 2003, Windows 2008, Windows 7, Windows 8.1.

Sentinel EMS Database


System	Supported Database Server Software
Windows	<ul style="list-style-type: none"> ■ Microsoft SQL Server 2005 x86/x64 ■ Microsoft, SQL Server 2005 Express Edition (must be enabled for remote connections) x86/x64 ■ Microsoft SQL Enterprise 2008 x86/x64 ■ Microsoft SQL Enterprise 2008 R2 x86/x64 <div>  Microsoft SQL Server 2008 R2 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. </div>

Web Browsers for Sentinel EMS


- Microsoft Internet Explorer versions 8, 9, 10
- Mozilla Firefox (32-bit) version 22
- Google Chrome (32-bit) version 23 or later

You must use a 32-bit Web browser for any action in Sentinel EMS that accesses a protection key (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"> ■ (x86 and x64) Windows XP, Windows Vista, Windows 7, Windows 8.1, Windows Server 2003, Windows 2008, Windows 2008 R2, Windows Server 2012 <p>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 or Windows Server 2012, you must install Microsoft .NET Framework 3.5. </div>
Mac	<ul style="list-style-type: none"> ■ Mac OS X 10.6.8 (32-bit and 64-bit) ■ Mac OS X 10.7.5 ■ Mac OS X 10.8.5
Linux	<ul style="list-style-type: none"> ■ OpenSUSE 12.3 (x86 and x86_64) ■ Red Hat EL 5.9, 6.4 (x86 and x86_64) ■ Ubuntu Server 10.04 (x86 and x86_64) ■ Ubuntu Desktop and Server 12.04 (x86 and x86_64) ■ Debian 6.0.x (x86 and x86_64) ■ CentOS 6.4 (x86 and x86_64) <p>The latest service packs and security updates must be installed.</p>

Code Samples

Sample	Support Considerations	
Sentinel Licensing API Sample	Programming Language	Tested Compilers
	AutoCAD	AutoCAD 2009, AutoCAD 2010
	C	Visual Studio 2012, Visual Studio 2008, Visual Studio 2005, C++ Builder, Developer Studio 2006
	C++	Visual Studio 2012, Visual Studio 2010, Visual Studio 2008, Visual Studio 2005, C++ Builder, Developer Studio 2006 <div> To compile the 64-bit samples using VS 2008, ensure that the 64-bit compiler package is installed when you install VS.</div>
	C#	Visual Studio 2010, Visual Studio 2008, Visual Studio 2005
	Delphi	Delphi 2007, Developer Studio 2006
	Java	Java Developer Kit 1.7 Java Developer Kit 1.6 Java Developer Kit 1.5
	Visual Basic	Visual Studio 6
	Visual Basic .NET	Visual Studio 2010, Visual Studio 2008, Visual Studio 2005
	4D	4D v11 for Mac OS and Windows
Sentinel Licensing API – C Sample for Mac OS X	Operating Systems supported: <ul style="list-style-type: none"> Mac OS X 10.6.8 Mac OS X 10.7.5 Mac OS X 10.8.5 	
Sentinel LDK Run-time Environment Installer API Sample	Programming Language	Tested Compilers
	MSC	Visual Studio 2008, Visual Studio 2005, Visual Studio 2010, Visual Studio 2012
	MSI	Wise Installer 7, Wise Installer 6.2 InstallShield 12 InstallShield 2012 Spring Note: The provided solution can only be used with InstallShield 2012 Spring or later.

Sample	Support Considerations	
Sentinel Activation API Sample	Programming Language	Tested Compilers
	C	Visual Studio 2003, Visual Studio 2005, Visual Studio 2008, Visual Studio 2010, Visual Studio 2012 Provided workspace may need to be converted for the VS version used.
Sentinel LDK Run-time Environment Installer for Mac OS X	Operating Systems supported: <ul style="list-style-type: none"> Mac OS X 10.6.8 (32-bit and 64-bit) Mac OS X 10.7.5 Mac OS X 10.8.5 	
Sentinel LDK Licensing API – 4D Sample for Mac OS X	Operating Systems supported: <ul style="list-style-type: none"> Mac OS X 10.6.8 (32-bit and 64-bit) Mac OS X 10.7.5 Mac OS X 10.8.5 Version of 4D supported: <ul style="list-style-type: none"> 4D v11 SQL 	
Sentinel LDK Licensing API – 4D Sample for Windows	Version of 4D supported: <ul style="list-style-type: none"> 4D v11 SQL 	
Sentinel Activation API	Operating Systems supported: <ul style="list-style-type: none"> Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 (32-bit and 64-bit) Windows 2000 (32-bit) 	
Sentinel Activation API for Mac	Operating Systems supported: <ul style="list-style-type: none"> Mac OS X 10.6.8 (32-bit and 64-bit) Mac OS X 10.7.5 Mac OS X 10.8.5 	
Sentinel Activation Sample for Java	Java version supported: JDK 1.6.	

Supported Versions for Windows CE

The Sentinel LDK Run-time Environment (version 5.95) and Envelope deliverables are supported for Windows CE versions 5.0 and 6.0.

Dropped Support

This section lists platforms which were supported in the past, but have not been tested with Sentinel LDK v.7.0. SafeNet will continue to accept queries for issues related to these platforms and will attempt to provide information to resolve related issues.

Platforms for End Users

Sentinel LDK Run-time Environment, Protected Applications

Testing for the following platforms for the Sentinel LDK Run-time Environment, and protected applications (with or without the Run-time Environment) has been discontinued:

Linux:

- Ubuntu Desktop 10.04 (x86 and x86_64)

Sentinel LDK Documentation

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

Documents

Sentinel LDK documents (PDF files) can be found:

- on the Sentinel LDK Installation DVD, under: **\Windows\Installed\Docs**
- where Sentinel LDK is installed, under:
...\Program Files (x86)\SafeNet Sentinel\Sentinel LDK\Docs
- where Sentinel EMS is installed, under:
...\Program Files (x86)\SafeNet Sentinel\Sentinel EMS\EMSServer\webapps\ems\Docs
 (For Win32, under **\Program Files\...**)

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>
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.

Document	Description
Sentinel HL Drive Flash Partitioning Utility – User Guide	Describes how to use the Sentinel HL Drive partitioning utility and API to load your Sentinel LDK-protected applications and data onto the CD-ROM partition of a Sentinel HL Drive, and ship it to your customers. Your customers can save files to Sentinel HL Drive or load additional software on it, and thus utilize the convenience of USB flash drive functionality.
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 - Sentinel HASP
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.

Help Systems - User Interfaces

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

Online Help System	Description
Sentinel LDK Admin Control Center	Documentation for the end user, describing the Admin Control Center and providing instructions for performing the various functions such as updating or attaching licenses.

Online Help System	Description
Sentinel EMS	Provides the Sentinel EMS user with detailed directions on how to set up license entities and how to handle entitlements, production, and support for Sentinel HL and SL keys.
Sentinel LDK Data Encryption Utility (Separate versions for Windows and for Mac)	Provides the developer with a description of the Sentinel LDK Data Encryption utility (formerly DataHASP utility), used for protecting data files that are accessed by Sentinel LDK Envelope.
Sentinel LDK Envelope (Separate versions for Windows and for Mac)	Describes how to employ Sentinel LDK Envelope to automatically wrap your programs with a protective shield. The application provides advanced protection features to enhance the overall level of security of your software.
Sentinel LDK ToolBox	Describes how to work with the ToolBox user interface for the Licensing API, License Generation API, and Admin API. Using Sentinel LDK ToolBox, the developer can experiment with the individual functions that are available in each API and can generate programming code for insertion in the developer's own program. Provides full documentation for each of the included APIs.

Online Help Systems - Sentinel LDK APIs

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

- on the Sentinel LDK Installation DVD, under: **\Windows\Installed\API**
- where Sentinel LDK is installed, under:
...\Program Files (x86)\SafeNet Sentinel\Sentinel LDK\API

(For Win32, under\Program Files\...)

Sentinel LDK API	Description
Activation API Reference	Together with various Licensing API functions, this API assists the developer in communicating with the Sentinel EMS Server.
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).

Sentinel LDK API	Description
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 ...\Program Files (x86)\SafeNet Sentinel\Sentinel EMS\EMSServer\webapps\ems\Docs\ (For Win32, under \Program Files\...)
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	Provides the functionality available in Admin Control Center and Sentinel License Manager in the form of callable API functions.

Software and Documentation Updates

SafeNet 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.7.0 that are likely to have the most significant impact on users are listed below, according to component.

Sentinel Vendor Suite Installation

Ref	Issue
133240	<p>When Installing Sentinel Vendor Suite under Windows 2003, the installation may fail with an internal error or with error messages similar to the following:</p> <p style="padding-left: 40px;">Error 1718. File <i>fileName</i> was rejected by digital signature policy. Installation ended prematurely because of an error.</p> <p>This problem is caused by a known issue in Windows 2003. To resolve this problem, go the following Microsoft URL: http://support.microsoft.com/kb/925336</p>
171812	<p>In a machine with an Nvidia graphics card and AMD64 processor, installation of Sentinel EMS may stop responding after the installer displays the "installed successfully" screen. At this point, installation of Sentinel EMS has succeeded, but the Finish button is not displayed, and the installer cannot continue with the installation of Sentinel Vendor Suite (if you requested to install it).</p> <p>Workaround: Perform the installation using a remote desktop. Alternatively, cancel the installation wizard when the "installed successfully" screen is displayed, and then run the installation wizard a second time and select only the Vendor Suite for installation.</p>
172141	<p>On a machine with a localized operating system, installation of Sentinel EMS in a directory whose name contains localized characters fails with "Error 1324".</p> <p>Workaround: Install Sentinel EMS in a directory whose name does not contain localized characters.</p>
180267 180270	<p>When Sentinel LDK is installed on a machine that connects to the Internet using a proxy, the update download may fail or may show incorrectly that updates are not available. This issue should resolve itself when the Software Manager application is automatically updated. Until this occurs, SafeNet recommends that you periodically check Sentinel Customer Community website for information on new available downloads.</p>

Sentinel EMS

Ref	Issue
EMSLDK-87 143768	<p>If Sentinel EMS is configured to work with a remote database that uses a password that contains non-English letters, Sentinel EMS Service fails to log in successfully to the remote database.</p> <p>Workaround: Change the password for the database so that it does not contain non-English letters.</p>

Ref	Issue
167309	In the RUS Branding screen, the list field for selecting the font does not work correctly in the Google Chrome browser. Workaround: Use a different browser to edit the RUS Branding screen.
182566	If you are viewing previous activations for "Protection Key Update Entitlement" and attempt to download V2C files for all the activations in that entitlement, the download will not succeed if more than 1,000 V2C files must be downloaded.
EMSLDK-4548	When you attempt to perform check-in for an empty legacy C2V file in Sentinel EMS, the action fails with the message: "At least one Feature or memory segment" Workaround: Perform check-in for the C2V file a second time. The action will succeed.

Sentinel LDK Master Wizard

Ref	Issue
139726	<p>Under some versions of OpenSUSE Linux, when the Master Wizard is run as root, the application hangs with the following output:</p> <pre>qctest@linux-g09j:~/Desktop/Linux/VendorTools/VendorSuite> su Password: linux-g09j:/home/qctest/Desktop/Linux/VendorTools/VendorSuite # ./masterhasp ** GLib-GIO:ERROR:gdbusconnection.c:2279:initable_init: assertion failed: (connection->initialization_error == NULL) Aborted</pre> <p>This appears to be the result of a known issue in OpenSUSE.</p> <p>Workaround:</p> <p>Enter the following commands to run the Master Wizard:</p> <pre>su - ./masterhasp</pre> <p>(Note the syntax: "su -")</p>
172697	<p>When the Master Wizard is run from the console under Debian 6.0, the following warning is displayed:</p> <pre>Qt: Session management error: None of the authentication protocols specified are supported</pre> <p>This message can be ignored. The Master Wizard performs its function correctly.</p>

Sentinel LDK Runtime Environment Installer

Ref	Issue
LDK-2916 (8475)	<p>When you attempt to integrate the Sentinel LDK Run-time Environment Installer MSM module in your Windows Vista installation package, a warning may be displayed. This is a known issue for the Installer, and the message can be ignored. For more information about this issue, go to the following URL:</p> <p>http://kb.flexerasoftware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=Q107955&sliceId=1&docTypeId=D T_ERRDOC_1_1&dialogID=95513399&stateId=0%200%2095503947</p>

Sentinel LDK Runtime Environment and Customer Tools

Ref	Issue
12506	Sentinel LDK communicates via TCP and UDP on port 1947. This port is IANA-registered exclusively for this purpose. At the end user site, the firewall must be configured so that communication via this port is not blocked.
140898	Under the Linux operating system, Sentinel License Manager does not support the IPV6 network protocol.
180256	When a computer names contains UTF-16 characters, Admin Control Center displays the short name for the computer (similar to Windows Explorer). Similarly, the sntl_admin_get function in Admin API returns the short name.
182646	<p>After Windows 7 is upgraded to Windows 8, the user may not be able to use existing SL licenses or to install new SL licenses.</p> <p>Workaround:</p> <p>After you upgrade from Windows 7 to Windows 8, reinstall the Run-time Environment</p>
LDK-2471	<p>Sentinel Licensing API: On a computer with the Nvidia chip set GeForce 7025/nForce 630a, and where the CPU is AMD Athlon 64 X2, the hasp_read and hasp_encrypt functions may fail with error 39, HASP_BROKEN_SESSION. This problem only exists with Sentinel HL keys with Firmware version 3.25.</p> <p>Workaround 1: On the computer described above, when error 39 is returned, call the hasp_read or hasp_encrypt function again. It is not necessary to call hasp_login again.</p> <p>Workaround 2: Use Sentinel HL keys with Firmware version 4.2x.</p>

Ref	Issue
LDK-2830	<p>Given the following scenario:</p> <ol style="list-style-type: none"> 1. An end user is working with a Linux virtual machine with active IPV6-supported network Ethernet adapters. 2. Using Sentinel LDK v.7.0 tools: The end user collects a fingerprint, and the vendor generates an SL license. The SL license is installed on the virtual machine. 3. The user disables networking (that is, Ethernet adapters are visible but not running) and restarts the virtual machine. <p>In Admin Control Center, licenses from Sentinel LDK 7.0 are shown as cloned. The licenses are not usable.</p> <p>Workaround: The end user should restart the hasplmd daemon, using: /etc/init.d/aksusbd restart</p>
LDK-2911	<p>For certain distributions of Linux (such as OpenSUSE), when networking is enabled on a Linux virtual machine: When the virtual machine is restarted, licenses are shown as cloned in Admin Control Center and become unusable.</p> <p>Workaround: The end user should restart the hasplmd daemon, using: /etc/init.d/aksusbd restart</p>

Sentinel LDK ToolBox

Ref	Issue
183073	<p>In the current release, Sentinel LDK ToolBox does not support the new <code>sntl_admin_context_new_scope()</code> function in the Admin API. However, the function appears in the Help system for Sentinel LDK ToolBox, and the function is supported by the Admin API.</p>

Sentinel LDK Envelope for Windows Platforms

General

Ref	Issue
92503	<p>If you move an Envelope project file from its original location to a different location, then the next time you open the project, Envelope displays an incorrect path for the output (protected) file.</p> <p>You can use either of these workarounds to move an Envelope project file to a new location:</p> <ul style="list-style-type: none"> ■ Use the Save As option from the Envelope File menu to save the project to the new location. (You can afterwards delete the original project file.). ■ Copy the directory structure containing both the project file and the related unprotected binary to the new location.

Ref	Issue
93877	(For Windows Vista and Windows 7) In the event that the error “Serious internal engine error (65535)” is displayed, make sure that you have write permission for the specified output directories and that the output directory is not protected by Windows UAC.
178432	<p>If the installation path for the Vendor Suite contains GB 18030 or Unicode characters, then the help file for Envelope, ToolBox, or Data Encryption utility does not open.</p> <p>This is Microsoft limitation. See the related article link: http://support.microsoft.com/kb/2606439</p> <p>Workaround: Manually open the help files after copying them from <code>\Windows\Installed\VendorTools\VendorSuite\translations\6.4</code> on the DVD to a location on your local hard drive whose path name does not contain GB 18030 or Unicode characters.</p> <p><i>OR</i></p> <p>Install the Vendor Suite in a location whose path name does not contain GB 18030 or Unicode characters.</p>
182883	<p>If the logon user name for Envelope contains multibyte UTF-8 characters: When the user attempts to protect an application, the error “Undefined engine error (1)” is generated.</p> <p>Workaround: Do not use multibytes UTF-8 characters in the logon user name.</p> <p><i>OR</i></p> <p>In the Envelope Settings screen (Advanced tab), select the option to use Legacy Envelope engines.</p>
183967	<p>If an Envelope project name contains Unicode characters, then while launching Data Encryption from Envelope, the message "Could not open project" is displayed.</p> <p>Workaround: Do not include Unicode characters in the Envelope project name.</p> <p><i>OR</i></p> <p>Do not launch Data Encryption from within Envelope. Instead, start the Data Encryption utility (datahasp.exe). In the Data Encryption utility, click New project and provide the path of the Envelope project.</p>
185624	<p>In the Protection Settings for a Windows DLL, you cannot select the option User debugger detection.</p> <p>Workaround:</p> <ol style="list-style-type: none"> Select the option Overwrite default protection settings. Save the project and close Envelope. Restart Envelope. <p>You can now select the option User debugger detection.</p>

Java

Ref	Issue
11043	To protect JAR files using Sentinel LDK Envelope on Windows 2008 Server 64-bit computers, you must have the Win32 Java Run-time Environment (JRE) installed, even if you already have the Windows x64 JRE installed. Alternatively, ensure that the path to the Windows x64 JRE is included in the system path variables.
91963 (CASE 20)	<p>When a (vendor) developer attempts to create a shared object file that links to the Sentinel LDK shared object file libhasp_linux_batchCode.so, error messages similar to the following are displayed:</p> <pre> user@host:~/Desktop/API/Runtime/Java/source> ./build_linux_x64.sh Building HASP Java native library /usr/lib64/gcc/x86_64-suse-linux/4.3/../../../../x86_64-suse- linux/bin/ld: HASPJava.o: relocation R_X86_64_32 against `a local symbol' can not be used when making a shared object; recompile with -fPIC HASPJava.o: could not read symbols: Bad value collect2: ld returned 1 exit status </pre> <p>This problem occurs because the Sentinel Licensing (Run-time) API was not compiled to allow position-independent code generation (using the -fPIC flag).</p> <p>Workaround: You can obtain a version of the Sentinel Licensing API that was compiled with the -fPIC flag. For more information, contact Technical Support.</p>
93464	<p>Envelope v.5.10 and Envelope v.6.0 both provide extensive enhancements for protection of Java programs. As a result, projects for Java programs that were created before the release of this version of Envelope must be updated using the Sentinel LDK Envelope GUI. (Make sure that you update existing Envelope projects as described below before you attempt to use the current Envelope command-line utility with these projects.)</p> <p>To update an existing Envelope project (v.5.10 or earlier) to v.6.0 or later:</p> <ol style="list-style-type: none"> 1. Open the project in the Sentinel LDK Envelope v.6.0 GUI and click the application in the Project pane. Envelope fills in the class/method list. By default, some methods are preselected. This is equivalent to the results expected when adding a new project. 2. Review the selection of methods that were selected by default for protection. For more information, see “Optimizing Protection Settings for Performance and Security” in the Sentinel LDK Envelope online help. 3. Save the project.

Ref	Issue
94373	One of the optional behaviors in Envelope for protecting JEE applications is to halt the thread if the protected JEE application fails to detect a Sentinel protection key. This behavior is controlled by the advanced protection property <code>SUSPEND_THREADS</code> . However, the protection mechanism also halts all threads from all third-party application running in the same Java Virtual Machine instance (JVM) on the Tomcat server. (Note that each Tomcat server only starts a single JVM instance.) Therefore, when protecting JEE applications in Envelope, the default value for the <code>SUSPEND_THREADS</code> property is currently set to False (although the documentation states that it is set to True). If you attempt to set the value for this property to True , a warning message is displayed.
95269	The current release of Sentinel LDK Envelope does not support protection of Java paint methods, but it allows you to select them in the user interface. As a result, the protected program may cause a deadlock when it executes a protected paint method at runtime with no Sentinel key connected. To prevent this issue from occurring, you can deselect all paint methods. Note that paint methods do not usually contain application logic; therefore, deselecting them typically has no impact on security. As an alternative, you can select console output for messages by enabling stderr output instead of windows in the Advanced settings panel.
95491	<p>The current release of Sentinel LDK Envelope does not support protecting instance methods that call instance methods of the super class. Note that such methods are not detected by the Envelope and may be selected for protection by default. As a result, the protected application may trigger an <i>IllegalAccessError</i> exception during runtime.</p> <p>To prevent such exceptions, you can disable the protection of methods that contain calls to super class methods. Note that this reduces the level of protection.</p> <p>As an alternative, you can create a new class with a method that contains only the code leading up to (but not including) the call to the super instance method. You can protect this method instead of protecting the original method that contains the super instance method call.</p>
104163 (99869)	<p>A protected JAR/WAR archive that contains Unicode characters in its path or name will not operate under the native operating system. Although there is small chance that the archive will run (depending on the type of Unicode characters that are used), in most cases the application will not run and will display an error message. (This problem does not occur on systems that use MUI for localization.)</p> <p>Workaround: Install the Tomcat server in a path whose name contains only ASCII characters. Ensure that the name of the WAR archive contains only ASCII characters.</p>
104179	<p>The number of instances of a protected application that can run in a network environment may exceed the number of concurrent instances allowed by the license terms.</p> <p>Workaround: In the protected application, call a Run-time API function to open a permanent session to the Feature for which concurrency is restricted.</p>
179821	The Java Envelope does not support unicode.

Ref	Issue
180073	When a protected Java application is executed, the execution counter is decremented once, and then decremented for each protected method. Therefore protected Java applications should not be licensed based on execution count.
180733	The current release of Envelope supports only one protected war file in a given JBOSS 7 Server.
181673	Legacy Envelope engines for Windows x86 and Windows x64 programs are not supported under Windows 8 (32-bit and 64-bit) or Windows 2012 Server.
LDK-2490	<p>If the protected application contains code similar to this:</p> <pre>List<User> function_name (Parameter) { ... }</pre> <p>After this method is protected with Java Envelope, Envelope will return a List variable that is not typecasted to the <User> type. This <User> type is another defined class in the same scope.</p>
LDK-2891	<p>The protected Java application directory should be set in the environment variable, or the classpath entry should be in the Manifest file of the original application.</p> <p>In fact, Java Envelope adds an entry for run-time required JAR files in the protected application Manifest file under the classpath tag. If the classpath tag did not exist in the original Manifest file, then these entry will not work. At run time, the protected Java application will search for run-time JAR files from the classpath environment variable. If the application does not find these run-time JAR files, it will throw “Class Not Exception” for these files.</p> <p>Work around 1: Add the current directory path to the classpath environment variable.</p> <p>Workaround 2: Modify the Manifest file to add the classpath tag.</p>
None	If protected JEE applications from multiple vendors are deployed on a single Tomcat server, the applications will not operate.

.NET

Ref	Issue
89873	If a base class is selected to be obfuscated and a derived class is not set to be obfuscated, the derived class will not find the base class. Therefore, if you select a base class for obfuscation, you must also select any derived class for obfuscation.

Sentinel LDK Envelope and Data Encryption for Mac OS X

Ref	Issue
11416	In certain instances, a protected Mach-O binary may have a different owner and permissions than it had prior to protection with Envelope. This is caused because Envelope designates the current user (that is, the user applying the protection) as the owner of the newly-created files.

Ref	Issue
132292	<p>Applications that use deprecated functions or classes (for example: NSQuickDrawView used by SDL, deprecated since OS X 10.4.x) might fail to run under Mac OS X 10.7.x after protection. This is the case even if the unprotected application executes correctly or if the protected application executes correctly under versions of Mac OS X prior to 10.7.x</p> <p>Workaround: Do not use SDL or any other Library/Framework that relies on deprecated System Frameworks.</p>
151020	<p>Given the following situation:</p> <ul style="list-style-type: none"> ■ An application is protected using Envelope with the Data Encryption facility enabled. ■ The protected application is operated under OS X 10.6.x or later with Versions feature enabled. <p>Encrypted files may become corrupted, resulting in data loss.</p> <p>Workaround: Handle data encryption/decryption manually without using the Data Encryption facility. You can use the <code>hasp_encrypt</code> and <code>hasp_decrypt</code> functions in the Sentinel Licensing API. For examples that use these functions, see the Runtime samples provided for Mac. Check the SafeNet website periodically for an updated version of the Envelope that resolves this issue.</p>
175314	<p>When protecting a Mac application, the following error message may be displayed: "Insufficient GAP for protection. Processing aborted"</p> <p>If this occurs, do one of the following:</p> <ul style="list-style-type: none"> ■ For Realbasic applications, use a newer version of Realbasic. In laboratory tests at SafeNet, the problem did not occur when working with Real Studio 2012 Release 2. ■ For other applications, pass suitable values to the -headerpad argument to ld, the static linker. For more details, refer to the documentation for ld, gcc or clang. You can add the option in the Other Linker Flags in the Linking section of the build settings in Xcode. <p>The headerpad option requires a size value in hexadecimal notation. For example, for one VM page, specify 0x4000. For more information, see the manpages ("man ld") description of headerpad size.</p> <p>Note: Some projects do not use ld directly, but link the application via gcc or clang.</p>
177241	<p>Applications that implement the symbols <code>malloc</code>, <code>calloc</code>, <code>free</code>, <code>realloc</code>, <code>dlopen</code>, <code>dlderror</code>, <code>dlsym</code>, or <code>dlclose</code> cannot be protected.</p>
183388	<p>An application may fail to run if it has been built with LDK static libraries using the Dead Code Stripping linking option.</p> <p>Workaround: Do not use the Dead Code Stripping option in linking.</p>

Sentinel LDK Envelope and Support for ARC in Mac OS X

ARC ("Automatic Reference Counting") is completely implemented by Apple in OS X as combination of:

- Special features of the clang compiler (ARC adds the code that had to be added by developers in the past).
- certain extensions to the Objective-C Runtime libraries.

Sentinel LDK Envelope for Mac sees an application using ARC as a standard application (since the missing code is created at compile time) interacting with an evolved backend (which is part of the operating system). As a result, Envelope supports applications that use ARC.

However, limitations exist as described in the explanation that follows.

Apple introduced ARC with OS X 10.7, so ARC is enabled in Xcode for OS X 10.7 (includes 10.7 SDK and clang supporting ARC). ARC is only available for 64-bit Mac applications. Apple also introduced a workaround to run ARC application under OS X 10.6.

The workaround is called *ARCLite*, as not all features are supported. ARCLite is a small static library that is linked to the developer application by default, at the time that the application is built with Xcode. This library basically extends the Objective-C runtime available under OS X 10.6 with the ARC feature.

In order to "inject" the ARC feature into pre-ARC Objective-C runtime, the ARCLite library (*libarclite*) contains code that is executed during initialization of the process *before* the original entry point is executed. Envelope cannot intercept this call. As the entry point has not been called, the code of libarclite (together with the application code) is still encrypted. As a result, the protected application fails.

Apple now uses ARCLite to extend older Objective-C runtime versions with new language features (new literals, indexed accessors in arrays and dictionaries) introduced as "modern Objective-C" in 10.8, even though these are unrelated to ARC.

Some applications that are linked with ARCLite fail after protection with Envelope, while others operate successfully. SafeNet is currently investigating this issue in order to obtain a clearer understanding of the problem.

Workaround

If an application that is linked with ARC fails after protection (especially when the application is started under the targeted OS X version, and not under the version under which the application was built), you can circumvent the issue by telling Xcode not to link ARCLite to the application. (As a result, certain new features possibly cannot be used on older platforms.)

To prevent Xcode from linking ARCLite, you must change the project/target settings. In the Xcode project settings pane, set the parameter **Implicitly Link Objective-C Runtime** to "NO".

This workaround generally prevents the protected application from failing. However, the workaround may cause issues when the application (with or without protection) is launched under older versions of OS X.

