Sentinel LDK – v.7.6

Release Notes

gemalto
security to be free

Revision History

Part number 007-013811-001, Rev A

Copyrights and Trademarks

Disclaimer

July 2017 Revision 1707-9

Contents

Sentinel LDK v.7.6 - 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=csm_index

- **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/

> Phone support is optionally available 24 x 7 x 365 when the user chooses to pay for the service. This is applicable to Sentinel LDK 7.6 products even where the associated documentation does not explicitly state this.

What's New in Sentinel LDK v.7.6?

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.7.5, 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.

Enhancements to Sentinel LDK Envelope

The enhancements described below have been implemented in Sentinel LDK Envelope.

AppOnChip Can Now Protect 64-bit Native Binaries

You can now use the AppOnChip feature in Sentinel LDK Envelope to protect both 32-bit and 64-bit native binaries (EXE and DLL files). In the current release, .NET assemblies are not supported.

For 64-bit native binaries, the Sentinel HL key used by AppOnChip must have firmware version 4.52 or later. Your customers can upgrade the firmware to the required version by applying the **firmware_update_453.v2c** file that you will find in one of these locations:

- On the Sentinel LDK Installation Drive, under **\Windows\Installed\Redistribute\Firmware Update\Sentinel HL**

- On the machine where Sentinel LDK is installed, under **%ProgramFiles(x86)%\Gemalto Sentinel\Sentinel LDK\Redistribute\Firmware Update\Sentinel HL**

To update the firmware on the HL (Driverless configuration) key, ensure that the end user receives the V2C file described above. The end user should do one of the following:

1. Connect the HL key to the machine where the Run-time Environment is installed. No other key should be connected to the machine.

2. In Admin Control Center, use the **Update/Attach** option to apply the V2C file to the HL key.

OR

1. Connect the HL key to the machine where the RUS utility is installed. No other key should be connected to the machine.

2. In the RUS utility, use the **Apply License Update** tab to apply the V2C file to the HL key.

Added Support for Linux ARM

Sentinel LDK Envelope for Linux (on a Linux Intel platform) can now protect applications that will run on ARM 32-bit and ARM 64-bit platforms.

Enhancements to Periodic Background Checks

The option for a protected application to perform periodic background checks for a Sentinel protection key has been enhanced. When the connection to a protection key is lost during a work session:

- The notification can now provide both **Retry** and **Abort** buttons.

- You can grant the user one or more grace periods to save work-in-progress and perform an orderly shut down of the application.

These enhancements are available in Sentinel LDK Envelope for Windows platforms (including .NET and Java), Sentinel LDK Envelope for Mac, and in Sentinel LDK Envelope for Linux platforms.

Added Support for SL UserMode Protection Keys in Linux Applications Protected With Sentinel LDK Envelope

Linux applications that are protected by Sentinel LDK Envelope can now be licensed with SL UserMode keys. This includes Linux Intel, Linux ARM 32 (EL and armhf) and Linux ARM 64 (aarch64).

Enhanced Support for Protection Against Debugger Detection and Memory Dump for Linux Applications

Shared objects in Linux applications (both 32-bit and 64-bit binaries) can now be protected against debugger detection and memory dumps with Sentinel LDK Envelope.

New Envelope Tool for the National Instruments LabVIEW Application

Sentinel LDK now provides a standalone envelope tool to protect the National Instruments LabVIEW application (RTEXE) running on cRIO-9030 or cRIO-9067 devices. These embedded devices run the NI Linux real-time operating system.

For more information, see the *Sentinel LDK Envelope for RTEXE - User Guide* in the documentation directory.

Enhanced Access Control for Admin Control Center and Admin API

In the past, Admin Control Center and Admin API provided a configuration parameter that determined whether a remote user could access and perform actions in Admin Control Center. However, this parameter did not control remote access to Admin API.

Now, the parameter **Allow Remote Access to ACC and Admin API** (in Admin Control Center) and the tag **<accremote>** (in Admin API) control remote access to both Admin Control Center and Admin API.

Additional Location for License Manager Configuration File

Until now, two specific locations were available to contain the configuration file **hasp_*vendorID*.ini** for the External and Integrated License Managers.

Effective with applications that are protected with Sentinel LDK 7.6, the configuration file can additionally be placed in the directory **%ProgramData%\Safenet Sentinel\Sentinel LDK**. If configuration files are present in multiple locations and contain conflicting information, preference is given to the files that occur first in the following list:

1. the default location

2. the application directory

3. the **%ProgramData%\Safenet Sentinel\Sentinel LDK** directory

For more information, see the description of the License Manager in the *Sentinel LDK Software Protection and Licensing Guide*.

Sentinel LDK Software is Now Provided on a Sentinel HL Drive microSD

Starting with Sentinel LDK v.7.6, Sentinel LDK software will be provided on a Sentinel HL Drive microSD instead of on a DVD.

> After you install Sentinel LDK, you have the option of replacing the Sentinel LDK microSD card in the Sentinel HL Drive key with your own microSD card. (Put the Sentinel LDK microSD card in a safe place in case you must install Sentinel LDK again.) You can then use the Sentinel HL Drive key as a sample for developing your own applications for delivery using this media.

Accessing Sentinel EMS From a Mac Machine

You can now access and perform actions in Sentinel EMS using the Google Chrome Web browser. Java applets are not used to access protection keys.

In the current version, Sentinel Remote Update System (RUS) is not supported for Mac. Alternative methods must be used to perform RUS functions.

New Clone Protection Scheme for Android Devices

A new clone protection scheme is now available for protected applications that are operated on Android devices.

The **PMType4** scheme provides clone protection similar to that offered by **PMType3**.

However, **PMType4** provides additional benefits for users who uninstall and then reinstall the protected application.

When reinstalling a protected application, the user is normally required to request a new V2C file from the vendor to re-enable the license for the application. This is required because some licenses may restrict the number of executions or may be time-restricted based on the installation date.

However, with the **PMType4** scheme, if the license is perpetual or is time-restricted based on an absolute expiration date, a new V2C file is not required. As a result, both the vendor and the customer are saved the effort of resolving licensing issues unnecessarily.

PMType4 is supported both by Sentinel EMS and by Sentinel License Generation API.

For more information about the **PMType4** clone protection scheme, see the *Sentinel LDK Software Protection and Licensing Guide*.

dfcrypt Utility Now Supports Version 2 Data Protection Mode

The **dfcrypt** utility can now be used to apply Version 2 protection to data files. This utility provides a command line-based alternative to the Sentinel LDK Data Protection utility for protecting data files.

For more information, see Chapter 7, "Protecting Data Files," in the *Sentinel LDK Software Protection and Licensing Guide*.

Enhanced Support for Integrated License Manager Under Linux

Under Sentinel LDK 7.5, the Integrated License Manager was supported only for applications that were protected using the Sentinel Licensing API. The Integrated License Manager and SL UserMode keys were not supported for applications that were protected using only Sentinel LDK Envelope.

For this release of Sentinel LDK, the Integrated License Manager and SL UserMode keys are now supported under Linux, both when using Sentinel Licensing API and when using the latest Sentinel LDK Envelope to protect your application.

Enhanced Support for SL UserMode Keys

Online Activation

SL UserMode keys can now be activated online using the Sentinel LDK Customer Portal.

SL UserMode Keys are Now Displayed in Sentinel Admin Control Center

SL UserMode keys can be used to license an application without installing the Run-time Environment on the machine. However, if the Run-time Environment was installed, the Sentinel Keys page in Admin Control Center on the machine would not display existing SL UserMode keys.

Starting with Run-time Environment v.7.60, Admin Control Center (under Windows) can display and apply updates to local SL UserMode keys. (Session information and certificate information for SL UserMode keys is not displayed.)

> To display SL UserMode keys, the License Manager runs an additional process (hasplmv) on the machine. The user has the option of disabling this process by clearing the relevant check box on the Configuration page in Admin Control Center. This would disable the ability to see SL UserMode keys.

Change to the Mac Customized RTE Installer in Sentinel EMS

In earlier versions of Sentinel LDK, the customized RTE installer that you could generate in Sentinel EMS was contained in the **Sentinel Runtime.pkg** file.

In this release, the customized RTE installer is provided in the signed file **SentinelRuntimeInstallerCLI**.

The structure of the files that the customized RTE Installer contains has been changed. As a result, it is no longer necessary to execute the Runtime Environment installer with **sudo** privileges.

What's Changed in This Release?

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

Documentation for Adding DigiCert for Device Guard

EMS users who are working in Web browsers that do not support Java applets now require Sentinel Run-time Environment on their machines. Sentinel EMS installs the Run-time Environment automatically for these users.

To install the Run-time Environment on a machine where Device Guard is enabled in enforce mode (which make use of PcaCertificate level code signing check), DigiCert must be listed/added in the Signers list of the policy file.

For information on how to accomplish this, see "Issues Related to Device Guard and Code Integrity Policies" in the Run-time Environment Installer readme file.

Activation of an SL License Now Uses an Existing Protection Key If Available

Prior to Sentinel LDK v.7.6, when a customer activated an SL license using the Sentinel EMS Customer Portal, the customer was always given the option to install the license in a new SL key.

Starting with this release, if the customer's machine contains one or more existing SL keys, the customer is not given the option to add a new SL key to contain the activated license. The customer must choose one of the existing SL keys to contain the license.

> Some software vendors may have been resolving false clone detection incidents by issuing a new product key to the customer. This method will no longer work, because the customer will not have the option of adding a new protection key when they activate the new Product license.
>
> The correct method to resolve a false clone detection incident is to send the customer a V2C file that contains a clear clone update for the existing protection key.

Tested Compilers for Java Envelope Configuration API Are Now Documented

The tested compilers for Java Envelope Configuration API are now documented in "Tested Compilers for Code Samples" on page 19.

Integrated License Manager Is No Longer Deprecated

Due to the increasing importance of the Integrated License Manager in the various implementations of Sentinel LDK, Gemalto has decided to retain the Integrated License Manager permanently. Therefore, the Integrated License Manager is no longer referred to as "deprecated" in the product documentation.

Default Value for MANAGE_EXCEPTIONS Parameter in Protected Applications Changed to "False"

The advanced protection parameter MANAGE_EXCEPTIONS in Sentinel LDK Envelope determines whether run-time exceptions in the protected application are handled by code injected by Envelope or by the Windows operating system. Until now, the default value for this parameter was "True".

Starting with applications protected using Sentinel LDK 7.6, the default value for this parameter is "False" (that is, run-time exceptions will be handled by the operating system).

Incorrect Information Regarding Support for Integrated License Manager Under Linux

The initial version of the release notes for Sentinel LDK 7.5 stated that the Integrated License Manager is supported under Linux for all protected applications. In fact, for Sentinel LDK 7.5, the Integrated License Manager was supported only for applications that were protected using the Sentinel Licensing API. The Integrated License Manager was not supported for applications that were protected using only Sentinel LDK Envelope.

For Sentinel LDK 7.6, the Integrated License Manager is supported under Linux both when using Sentinel Licensing API and when using Sentinel. LDK Envelope to protect your application.

Corrections to Product Documentation

The product documentation has been corrected as described below.

Paths for License Manager Configuration Files Have Been Corrected

The paths for configuration files for the Integrated/External License Managers are provided in the *Sentinel LDK Software Protection and Licensing Guide*. In version 7.5 of the book (on page 189), the paths incorrectly contained the directory *Gemalto Sentinel* instead of *SafeNet Sentinel*. The paths have been corrected in the latest version of the book and are also provided below.

Type of application	Default Location
Desktop (Windows Vista/7 or later)	*%LocalAppData%\SafeNet Sentinel\Sentinel LDK*

Type of application	Default Location
Desktop (Windows XP)	*%UserProfile%\Local Settings\Application Data\SafeNet Sentinel\Sentinel LDK*
Service (**Local Service** account) x64 operating system	*%systemroot%\SysWOW64\config\systemprofile\AppData\Local\SafeNet Sentinel\Sentinel LDK*
Service (**Local Service** account) x86 operating system	*%systemroot%\System32\config\systemprofile\AppData\Local\SafeNet Sentinel\Sentinel LDK*
Service (**Network Service** account)	*%systemroot%\ServiceProfiles\NetworkService\AppData\Local\SafeNet Sentinel\Sentinel LDK*

Paths for the V2C Files for SL Licenses Have Been Corrected

The paths for V2C files that have been applied to update SL licenses under Windows have been corrected in the *Sentinel LDK Software Protection and Licensing Guide*. In version 7.5 of the book (on page 144), the paths incorrectly contained the directory *Gemalto Sentinel* instead of *SafeNet Sentinel*. The paths have been corrected in the latest version of the book and are also provided below.

SL AdminMode	*%ProgramFiles(x86)%\Common Files\Safenet Sentinel\Sentinel LDK\installed\ [vendorID]*
SL UserMode	*%ProgramData%\SafeNet Sentinel\Sentinel LDK\installed\[vendorID]*

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 7.60
Mac	Version 7.60
Linux Intel	Version 7.60

> 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	■ Windows 7 SP1 ■ Windows 8.1 SP1 ■ Windows Server 2008 R2 SP1 ■ Windows Server 2012 R2 ■ Windows Server 2016 ■ Windows 10 Version 1703 > Windows 10 Insider Preview builds are not supported. The latest service packs and security updates must be installed.
Windows Embedded	■ (x86 only) Windows 7 SP1 Embedded standard
Mac	■ Mac OS X 10.10 ■ Mac OS X 10.11 ■ Mac OS X 10.12 > The Sentinel Remote Update System (RUS utility) is not supported for Mac systems in this release.

System	Supported Versions	
Linux	**Linux Intel (x86 and x86_64)**	- OpenSUSE 12.3 - Red Hat EL 6.7, 7.2 - Ubuntu Server 14.04, 16.04 - Ubuntu Desktop 16.04 - Debian 8.x - CentOS 7.2 The latest service packs and security updates must be installed.
	Linux ARM 32-bit (armel and armhf)	The following hardware/boards have been validated: - BeagleBoard-xM Rev C - BeagleBone Black - Raspberry Pi-2 - PandaBoard ES Rev B3_ - NI cRIO-9068
	Linux ARM 64-bit (arm64)	The following hardware/board has been validated: Qualcomm DragonBoard 410c
	Wine	Sentinel LDK Run-time Environment was tested on Linux platforms with Wine 1.7.28.
Android	**Android ARM (32-bit) Android x86 (32-bit)**	Android 4.4.2, 5.1.1, 6.x
	Android Architecture	The following architecture is supported: - armv7 - armv7a - x86
	Android ABI	Sentinel LDK Envelope supports Android applications designed for the following Android application binary interfaces: - armeabi - armeabi-v7a - x86

System	Supported Versions
Virtual Machines	The VM detection and VM fingerprinting capabilities provided by Sentinel LDK have been validated on the following technologies: ■ Parallel Desktop 12 for Mac ■ VMware Player 6.0.3 (Free for non-commercial use) ■ VMware Workstation 12.x ■ VMware ESXi 5.5 ■ Hyper-V Server 2016 ■ Xen 4.6 ■ KVM (RHEL 7.2, Ubuntu 14.04 server, Debian 8.x) ■ Microsoft Azure **Note:** Azure stop/start is not supported at this stage and will cause the license to be flagged as cloned. ■ VirtualBox 5.1.x **Note:** An application that has been protected for performance profiling (with AppOnChip) will not work correctly with earlier versions of Virtual Box.

Data File Protection Plugin for Internet Explorer

The Data File Protection plugin (MSI file) is compatible with the following versions 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) versions 10, 11

■ Microsoft Edge

■ Mozilla Firefox - latest version

■ Google Chrome version 53 or later

■ Safari - latest version

Supported Platforms for Vendors

Sentinel EMS Service

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

Sentinel EMS Database

System	Supported Database Server Software
Windows	■ Microsoft SQL Enterprise 2008 x86/x64 ■ Microsoft SQL Enterprise 2008 R2 x86/x64 ■ Microsoft SQL Server 2012 x86/x64 ■ Microsoft SQL Server 2012 R2 x86/x64 ■ Microsoft SQL Server 2014 x86/x64 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. Although Microsoft SQL Server 2008 R2 Express Edition is not officially supported by Microsoft on Windows 10, it has been tested with Sentinel LDK 7.6. Gemalto recommends that you use Microsoft SQL Server 2012 or later in production environments. For detailed instructions on how to install and configure SQL Server 2012 for Sentinel EMS, see the Technical Note available here.

Web Browsers for Sentinel EMS

■ Microsoft Internet Explorer versions 10, 11

■ Mozilla Firefox version 40 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 30.

■ Google Chrome version 53 or later

> The Mac Safari Web browser is *not* supported for Sentinel EMS 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	■ See supported Windows platforms for Sentinel LDK Run-time Environment (above). Requires screen resolution 1280 by 1024 pixels with 24-bit color quality 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. 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.
Mac	■ Mac OS X 10.11 ■ Mac OS X 10.12 Applications built on the Cocoa framework are supported.
Linux Intel	■ OpenSUSE 12.3 (x86 and x86_64) ■ Red Hat EL 7.2 (x86 and x86_64) ■ Ubuntu Server 16.04 (x86 and x86_64) ■ Ubuntu Desktop 16.04 (x86 and x86_64) ■ Debian 8.x (x86 and x86_64) ■ CentOS 7.2 (x86 and x86_64) The latest service packs and security updates must be installed.
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	Sentinel Envelope supports Android applications designed for the following versions: 4.4.2, 5.1.1, 6.x Android ARM and x86 platforms are supported. (MIPS platform is not supported.)
Java	Sentinel LDK Java Envelope Configuration API

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 2010, 2013, 2015 C++ Builder Developer Studio 2006
	Visual Basic .NET	Microsoft Visual Studio 2013, 2015
	C#	Microsoft Visual Studio 2013, 2015
	C++	Microsoft Visual Studio 2010, 2013, 2015 C++ Builder Developer Studio 2006 GCC
	Delphi	Delphi 2007 Developer Studio 2006 Delphi XE3
	Java	Java Developer Kit 1.7,1.8
Licensing API for Mac OS X	Java	Java Developer Kit 1.7, 1.8
	C	GCC, Xcode
Licensing API for Linux	Java	Java Developer Kit 1.7, 1.8
	C	GCC
	C++	GCC
Licensing API for Android	Java	Java Developer Kit 1.8
License Generation API	C, C#, Visual Basic .NET	Microsoft Visual Studio 2013, 2015
	Java	Java Developer Kit 1.8
Activation API for Windows	C	Microsoft Visual Studio 2010, 2013, 2015 Provided workspace may need to be converted for the VS version used.
	Java	Java Developer Kit 1.7, 1.8
Activation API for Mac OS X	Java	Java Developer Kit 1.7, 1.8
Activation API for Linux	Java	Java Developer Kit 1.7, 1.8

API	Programming Language	Tested Compilers
Runtime Environment Installer	C	Microsoft Visual Studio 2010, 2013, 2015
	MSI	Wise for Windows Installer 7.1 InstallShield 2012 Spring or later **Note:** The provided solution can only be used with InstallShield 2013 Spring or later.
Admin API for Windows	Java	Java Developer Kit 1.8
	C, C#, C++, Visual Basic .NET	Microsoft Visual Studio 2013, 2015
Admin API for Linux	C	GCC
Admin API for Mac OS X	C	GCC, Xcode
Envelope .NET Runtime API	C#	Microsoft Visual Studio 2010, 2013, 2015 **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 1.7, 1.8

Supported Platforms for Sentinel Cloud Licensing

Sentinel Cloud Run-time has been tested on the following platforms:

Run-time	Run-time Interface	Platforms Tested	Run-time Environment	Web Server
Cloud	Java	**Windows** ■ Windows 2012 ■ Windows 8 ■ Windows 8.1 ■ Windows 7 ■ Windows Server 2008 **Linux** ■ Ubuntu 14 ■ CentOS 5.4 ■ Red Hat Enterprise Linux (RHEL) 6.3 ■ SLES 12.1	JRE 7.0	Tomcat 7
	.NET	**Windows** ■ Windows 2012 ■ Windows 8 ■ Windows 8.1 ■ Windows 7 ■ Windows Server 2008	.NET Framework 2.0 and 3.5	IIS 6.0 and 7.0
	C	**Windows** ■ Windows 2012 (64-bit) ■ Windows 8.1 (64-bit) ■ Windows 8 (64-bit) ■ Windows 7 (32-bit and 64-bit) ■ Windows Server 2008 (32-bit and 64-bit) **Linux (32-bit and 64-bit)** ■ Ubuntu 14 ■ CentOS 5.4 ■ Red Hat Enterprise Linux (RHEL) 6.3 ■ SLES 12.1	-	-

Run-time	Run-time Interface	Platforms Tested	Run-time Environment	Web Server
On-premise	Java	**Windows** ■ Windows 2012 (64-bit) ■ Windows 8.1 (64-bit) ■ Windows 8 (64-bit) ■ Windows 7 (32-bit and 64-bit) ■ Windows Server 2008 (32-bit and 64-bit) **Linux** ■ Ubuntu 14 ■ CentOS 5.4 ■ Red Hat Enterprise Linux (RHEL) 6.3 ■ SLES 12.1	JRE 7	Tomcat 7
	.NET	**Windows** ■ Windows 2012 ■ Windows 8 ■ Windows 8.1 ■ Windows 7 ■ Windows Server 2008	.NET Framework 2.0 and 3.5	IIS 6.0 and 7.0
	C (32-bit and 64-bit)	**Windows** ■ Windows 2012 (64-bit) ■ Windows 8.1 (64-bit) ■ Windows 8 (64-bit) ■ Windows 7 (32-bit and 64-bit) ■ Windows Server 2008 (32-bit and 64-bit) **Linux (32-bit and 64-bit)** ■ Ubuntu 14 ■ CentOS 5.4 ■ Red Hat Enterprise Linux (RHEL) 6.3 ■ SUSE 12.1	-	-

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)	Version of Firmware on Sentinel HL (HASP Configuration Keys)
7.6	4.53	4.33
7.5	4.27	4.27

To view 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 and open Admin Control Center.

Dropped Support

This section lists platforms and compilers that were supported in the past, but have not been tested with Sentinel LDK v.7.6. 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 Developers and End Users

Testing for the following platforms has been discontinued:

Platform	Discontinued For
4D Compiler	Vendors
Mac OS X 10.9.x	Vendors and end users
Mac OS X 10.10.x	Vendors
Microsoft SQL Server 2005	Vendors
Windows 2008 Server	Removed from documentation, no longer tested
Visual Studio 2008	Vendors
Windows CE	End users
Windows XP Embedded	End users
Windows XP, Vista, 2003 Server	Vendors and end users

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	Guide you through the basic procedures of Sentinel LDK to familiarize you with the applications and their functionality. • 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. Two versions of each tutorial are provided – one for working with Sentinel EMS as the back office system, and one for vendors who want to provide their own back office system and only use the Sentinel LDK APIs to handle licensing and protection.
Sentinel LDK Quick Start Guides	Provides a short and simple demonstration of how you can easily protect your software using Sentinel HL keys. Separate Demo Kit and Starter Kit guides are provided.
Migration Guide: Sentinel HASP to Sentinel LDK	Describes how to migrate from Sentinel HASP to Sentinel LDK. Describes how to migrate your Business Studio Server database to a Sentinel EMS database. This guide also describes the Business Studio Server API for Sentinel EMS.

Document	Description
Additional Guides for Migrating to Sentinel LDK	These guides describe how to migrate to Sentinel LDK from: - Hardlock - SmartKey - Sentinel SuperPro - HASP HL - HASP4 - Sentinel Hardware Keys
Integrating Sentinel EMS Server into Your Existing Back-Office Systems	Outlines the many ways that software vendors can maximize the potential of their existing back-office systems, such as ERP, CRM, and business intelligence systems, through seamless integration with Sentinel EMS Server.
Sentinel EMS Configuration Guide	Provides information on setting up and configuring Sentinel EMS to satisfy the requirements of your organization.
Sentinel EMS User Guide	Provides the Sentinel EMS user with detailed directions on how to set up license entities and how to handle entitlements, production, and support for Sentinel HL and SL keys. (This information is also provided in online help for the Sentinel EMS user interface.)
Sentinel EMS Web Services Guide	Provides the developer with an interface for integrating Sentinel EMS functionality into the vendor's existing back-office systems.

Sentinel Cloud Licensing Documents

The documentation in the table that follows describes how to work with Sentinel Cloud Licensing. This documentation is provided with the Sentinel Cloud Licensing installer.

Document	Description
Sentinel Cloud Run-time Guide	Sentinel Cloud Run-time API reference (Java, .NET, and C)
Sentinel Cloud - Quick Start Guide	Document to help you quickly start with Sentinel Cloud
Sentinel Cloud Services Installation Guide	Describes how to install Sentinel Cloud Services
Sentinel Cloud Connect Web Services Guide	Reference for using the Sentinel Cloud Connect Web services
Sentinel Cloud Run-time Java Demo Application ReadMe	Explains how to use the Sentinel Cloud Services Demo Application
Sentinel Cloud Run-time .NET Reference Application ReadMe	Sample for using the Cloud Runtime APIs written in .NET

Document	Description
Sentinel Cloud Run-time C Reference Application ReadMe	Sample for using the Cloud Runtime APIs written in C
Sentinel Cloud Connect Web Services Python Sample ReadMe	Sample for integrating Sentinel Cloud Connect Web services in Python application

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.

Online Help System	Description
Sentinel LDK Envelope (Separate versions for Windows and for Mac)	Describes how to employ Sentinel LDK Envelope to automatically wrap your programs with a protective shield. The application provides advanced protection features to enhance the overall level of security of your software.
Sentinel LDK ToolBox	Describes how to work with the ToolBox user interface for the Licensing API, License Generation API, and Admin API. Using Sentinel LDK ToolBox, the developer can experiment with the individual functions that are available in each API and can generate programming code for insertion in the developer's own program. Provides full documentation for each of the included APIs.

Online Help Systems – Sentinel LDK APIs

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

- On the Sentinel Customer Community web site, at:
  https://sentinelcustomer.gemalto.com/Documentation_Information.aspx

- on the Sentinel LDK Installation Drive, under: **\Windows\Installed\API**

- where Sentinel LDK is installed, under:
  %ProgramFiles(x86)%\Gemalto Sentinel\Sentinel LDK\API

  (For Win32, under: **%ProgramFiles%**…)

Sentinel LDK API	Description
Activation API Reference	Provides function calls that can be used to simplify the process of SL key activation at the customer site. (Deprecated – replaced by Sentinel EMS Web Services.)
Licensing API Reference (formerly Run-time API)	Provides the developer with an interface to use the licensing and protection functionality available in the Sentinel LDK Run-time Environment.
Run-time COM API	Provides the developer with access to Sentinel HASP Run-time Environment functionality, through an interface written for the Microsoft Component Object Model (COM).
Run-time Installer API	Provides the developer with an interface for integrating installation of the Run-time Environment into the installation of the vendor's protected application.

Sentinel LDK API	Description
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.7.6 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	Installation of Sentinel LDK on a virtual machine may hang before completion of the installation process. **Workaround:** Interrupt and then restart the installation. If the problem occurs again, interrupt the installation. Enable 3D acceleration and increase the video memory of the virtual machine. Rerun the installation.
LDK-12131	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).
EMSLDK-7448	Sentinel EMS fails to install correctly on a machine where JRE 8 and earlier versions of JRE coexists. If a machine contains an earlier version of JRE, and you manually install JRE 8, then: 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. 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. **Workaround:** Uninstall the earlier versions of JRE from your machine, and restart the Sentinel EMS installation. - 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.
EMSLDK-7806	If you accept the default SQL server (Microsoft SQL Server 2008 R2 Express Edition) provided by the Sentinel EMS installer, the installation fails under Windows 10 because this SQL server is not supported under Windows 10. **Workaround:** Before you install Sentinel EMS, install Microsoft® SQL Server® 2012 Service Pack 2 (SP2) Express. For detailed instructions on how to install and configure MSQL Server 2012 for Sentinel EMS, see the Technical Note available here.
LDK-16617	When the Windows Installer on the machine is version 4.0, the Sentinel EMS installation wizard fails to install SQL server 2008. **Workaround:** Restart the machine and start Sentinel EMS installation again.

Sentinel EMS

Ref	Issue
EMSLDK-5168	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. **Workaround:** When generating the RTE installer in Sentinel EMS, use the locking type **SL-AdminMode** for Products.
SM-11279	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/ **Workaround:** Create an exclusion for Edge to allow localhost loopback as follows: 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 (Amin) window is displayed. 3. Copy and paste the following command to the Command Prompt window, and press Enter: `CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"` Edge will now work correctly with Sentinel EMS.

Sentinel Cloud Licensing

Ref	Issue
EMSLDK-5934	Entitlement-level Caching: Sentinel Cloud Licensing is unable to consume a license if the end user machine contains multiple hard disk drives. Error 1021 is generated.

End Users, Sentinel LDK Runtime Environment, License Manager, and Customer Tools

Ref	Issue
LDK-8480	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.) **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().

Ref	Issue
LDK-9044	Given the following circumstances: ■ A Sentinel HL (Driverless configuration) key is connected to a USB host controller in default mode on QEMU emulator version 2.0.0 and Virtual Machine Manager version 0.9.5. When the key is disconnected, the key continues to be displayed in Admin Control Center as a connected key. (However, a protected application whose license is located in the key does not execute after the key is disconnected.) **Workaround:** Switch the USB controller to USB 2.0 mode.
LDK-10670	After a user connects a Razer Abyssus mouse and installs Razer drivers on a computer, the device manager on the computer does not recognize a Sentinel HL key if the key is connected to the same USB port where the mouse was previously connected. This issue has been reported to Razer.
LDK-12172	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. **Workaround:** Use the 32-bit Internet Explorer to view protected data files.
LDK-12547	Under Linux, if the user is running a Windows 64-bit protected application using Wine with default options, Linux may return a "debugger detected" error. **Workaround:** When you protect the application using Envelope, disable **User debugger detection** for the application.
LDK-14971	Given the following circumstances at a customer site: ■ One machine has Run-time Environment version 7.51. ■ A second machine has a version of Run-time Environment that is earlier than 7.51. ■ The customer performs rehost of a license repeatedly between the two machines. ■ An update is applied to the license on either of these machines. A rehost operation may fail with the message HASP_REHOST_ALREADY_APPLIED. **Workaround:** Obtain a new SL license from the software vendor for the protected application on the target machine. Before attempting any additional rehost procedure, install the latest Run-time Environment on both machines.
LDK-15991	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. **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.

Ref	Issue
SM-546	Given the following circumstances: ■ 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) The protected application may fail. **Workaround:** Include the External License Manager (hasp_rt.exe) with the protected application.
SM-10843	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: ■ 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: ■ If the application contains JARs within a JAR/WAR executable, remove those JARs when protecting the executable with Envelope. You can add the JARs to the JAR/WAR executable after protection is complete. ■ Create a JAR/WAR executable using only those classes that you want to protect. After applying protection, you can add other classes or JARs, or any other dependencies in the protected JAR/WAR executable.
LDK-11418	For a Java 7 or Java 8 application that is protected with Envelope, the end user must use the following flag when launching the protected application: ■ For Java 7: Specify `-usesplitverifier` ■ For Java 8: Specify `-noverify` If the appropriate flag is not specified, the application may throw **java.verifyerror** when launched.
SM-10890	Given the following circumstances: ■ An Envelope project was created with Envelope version 7.3 or earlier. ■ The project contains settings for a Java application. ■ On the **Protection Settings** tabbed page for the Java application, you select the option to overwrite default protection settings. The **Allows grace period after failed license check** check box should be modifiable. However, the check box cannot be changed. **Workaround:** On the **Advanced** tabbed page, make any change to the MESSAGE_OUTPUT_MODE property, and then change it back. This forces Envelope to load an internal data structure that then makes the **Allows grace period after failed license check** check box modifiable.
SM-10969	Due to a known limitation in Java, if a background check thread becomes non-EDT, the background check (**Abort/Retry/Ignore**) dialog box may not appear. Envelope has been modified so that the error dialog prompted by the protected method in the protected application takes precedence. This has reduced the occurrence of the problem, but it has not eliminated the problem entirely.

.NET

Ref	Issue

SM-554	For apps that target the .NET Framework version 4.6 and later, **CultureInfo.CurrentCulture** and **CultureInfo.CurrentUICulture** are stored in a thread's **ExecutionContext**, which flows across asynchronous operations. As a result, changes to the **CultureInfo.CurrentCulture** and **CultureInfo.CurrentUICulture** properties are reflected in asynchronous tasks that are launched subsequently.
	
	 If the current culture or current UI culture differs from the system culture, the current culture crosses thread boundaries and becomes the current culture of the thread pool thread that is executing an asynchronous operation.
	
	 When protecting a sample application implementing above behavior with protection type as "Dot Net Only", then the application behaves as expected. However, with protection type "Dot Net and Windows Shell" or "Windows Shell Only", the thread uses the system's culture to define behavior.
	
	 Workaround:
	
	 Do the following:
	
	 1. Use .NET Framework 4.5.
	
	 2. Use
	
	     CultureInfo.DefaultThreadCurrentCulture = new CultureInfo(...)
	
	 instead of
	
	     Thread.CurrentThread.CurrentCulture = new CultureInfo(...).

Sentinel LDK Envelope and Data Encryption for Mac OS X

Ref	Issue
LDK-11655	■ When running Envelope in a VMware Fusion 7.1.1 virtual machine on a Mac machine, if you save the protected application to 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.