New Features, Enhancements, and Changes

> **NOTE** If you are upgrading from a version of Sentinel LDK that is earlier than 9.0, be sure to review the release notes for all intervening versions. Significant enhancements and changes are introduced in each version of Sentinel LDK. Download a ZIP file that contains all Sentinel LDK release notes to see the changes.

Service Pack: 10.0.300

Fingerprint Generator Tool and API

Sentinel LDK now supports the generation of a machine fingerprint for machines in situations where outgoing file transmission is restricted (for example, for air-gapped machines).

A user can determine the required hardware identifiers data for generating a license on the target machine and share the data with you by telephone or email. You enter the provided data in to the Fingerprint Generator Tool (on a Windows machine) or the Fingerprint Generator API (on a Linux ARM64 machine) to generate a C2V file. The C2V file can then be passed to Sentinel LDK-EMS, which will use the C2V to generate a V2C or V2CP file to install an SL AdminMode or SL UserMode license on the target machine.

The user can provide one or more of the following hardware identifiers for generating the license:

- MAC address
- FQDN (Fully Qualified Domain Name)
- IP address
- SID (Security Identifier on Windows or System ID on Linux)

The Fingerprint Generator API enables you to:

- Support environments where C2V files cannot be shared due to security restrictions.
- Generate fingerprints that are compatible with both Windows and Linux platforms.
- Generate fingerprints for both physical machines and virtual machines.

For more information, see Sentinel LDK Software Protection and Licensing Guide.

Licensing API Returns Hardware Identifiers for Fingerprint Generation

To use the Fingerprint Generator Tool or API, you must obtain one or more of the following hardware identifiers from the user's machine: Mac address, FQDN, IP address, SID.

To simplify the process of determining the values for these identifiers, you can include a call to the Sentinel Licensing API getInfo function in the protected application on the user's machine. This function will determine the values for these identifiers. The user can then transmit these values to you using, for example, email or telephone.

The value provided by the getInfo function for each identifer will include a checksum. You can include this checksum when entering the value in the Fingerprint Generator Tool. The Tool uses the checksum to verify that the value was entered correctly. (Use of the checksum is not supported by the Fingerprint Generator API.)

For details, see Sentinel Licensing API C Reference.

The Licensing API Config Function Is Now Supported for Android

Automatic detach to SL-UserMode from an Android client is now supported. On-demand detach is not supported.

Reduced Load Time for Multiple DLLs Protected by Sentinel Licensing API

Sentinel LDK Licensing API has been enhanced to use a single instance of the hasp_rt.exe external license manager for multiple instances (for example, different DLLs) in a process. As a result, the load time (especially for Envelope-protected modules) has been reduced.

Disabling Secure Storage ID Check

By default, when an application attempts to log in to a Feature, the Secure Storage ID (SSID) is checked in a number of instances.

You can disable this check by including the <ignore_secure_storage_id_check> tag in the license. For details, see the topic "How to disable Secure Storage ID Check" in the Sentinel License Generation API Reference.

You can also disable this check when using the Fingerprint Generator Tool or Fingerprint Generator API

Enhancements to Sentinel LDK Envelope

The following enhancements to Sentinel LDK Envelope have been implemented in this release:

- **Display information log message when switching between V3 and NG engines**

  Switching between the V3 and NG protection engines for Windows applications now generates an information message in the log pane in the Envelope GUI.

  Note that switching the protection engine only affects files that are added to the Envelope project after the switch occurs. Existing files that are open in Envelope when the switch occurs are not affected.

  The message is only displayed if at least one file already exists in the ccurrent project in Envelope.

- **Windows Shell protection now generates a warning when protecting an assembly in "Any CPU" configuration**

  Given the following circumstances:

  - You are developing a .NET assembly and are using the Windows Shell protection in Envelope.
  - The assembly was compiled with the default “Any CPU” configuration.

  You now receive a warning that the Shell protection has bound the CPU configuration of the assembly to the x86 architecture. The protected binary can only be used in an x86 process.

  To avoid generating this warning each time you protect the application, compile the assembly using either the x86 or the x64 CPU configuration. The protected application can then be used only with an x86 process or only with an x64 process, depending on the CPU configuration used.

The Term "Identity-Based" Licensing Is Now "Device-Based" Licensing

The terms "identity-based" licensing and "identity string-based" licensing have been changed to "device-based" licensing.

The purpose of this change is to contrast between "user-based" licensing, where the user is authorized to use a license, and "device-based" licensing, where the device is authorized to use a license. This change has been implemented in Sentinel LDK and Sentinel EMS.

Service Pack: 10.0.200

- Modifications to PMType4 Documentation
- Licensing API Now Supports Detaching a License to an SL UserMode Key
- A Detached License for Cloud Licensing Can Now Be Limited to One Machine
- A Cloud License Can Now Support Multiple Sessions for an Identity on Multiple Machines
- The License Manager Access and Error Log Files Now Support JSON Format
- Sentinel Licensing API Now Supports Alpine Linux
- Enhancements and Changes for Sentinel LDK Envelope

Modifications to PMType4 Documentation

Documentation for the PMType4 clone protection scheme has been modified by addition of the following note:

> When using the PMType4 clone protection scheme:
>
> - To allows re-installation of a license on an Android device, **Rehost** should be disabled.
> - For keys that were produced before installing Sentinel LDK 10.0.100, it may still be necessary to send the user a new V2C file if they uninstalled and then reinstalled the app.

Licensing API Now Supports Detaching a License to an SL UserMode Key

You can now use the native Sentinel Licensing API to detach a license from an SL AdminMode key or CL key to an SL UserMode key. As a result:

- A license can be detached for a UBL user.
- A license can be detached from a SL AdminMode key on a local network or from a Thales-hosted or vendor-hosted cloud license.
- A license can be detached to any of the following platforms: Linux Docker, Linux, Windows
- The machine to which a license is detached does not require the Run-time Environment.
- Both auto-detach and on-demand detach are supported.

To use the detached license under these circumstances, an application must be protected using a vendor-specific API version 10.13 or later.

> **NOTE** To enable an application protected with Envelope to run using an SL UserMode key that was automatically detached, the following limitation applies: When protecting the application, the LOCKING_TYPE protection parameter must be set to **HL or SL (AdminMode or UserMode)** . (The default setting for this parameter is **HL or SL-AdminMode**.)

For details, see Sentinel Licensing API C Reference.

A Detached License for Cloud Licensing Can Now Be Limited to One Machine

By default, a license that is detached automatically from a cloud license on a vendor-hosted license server is now be limited to usage on a single machine.

You can remove this limitation by changing a configuration parameter in the INI file for the License Manager service. For details, see Sentinel Admin API C Reference.

A Cloud License Can Now Support Multiple Sessions for an Identity on Multiple Machines

A cloud license consumed by an identity can be shared by multiple sessions on multiple machines. This enables, for example, multiple Docker containers on a given machine or on multiple machines to use the same identity.

You can configure the License Manager service (LMS) hosted in trusted storage to allow multiple machines to log in to the cloud-enabled SL key using a single identity. For details, see Sentinel Admin API C Reference.

The License Manager Access and Error Log Files Now Support JSON Format

You can now configure Admin License Manager to generate log messages in JSON format. This can be configured by assigning the value 1 to the parameter jsonlog in the License Manager configuration file. For example:

```
jsonlog = 1
```

Sentinel Licensing API Now Supports Alpine Linux

Sentinel Licensing API is now compatible with software that uses Docker and Alpine Linux on Linux Intel x86_64 platform.

Enhancements and Changes for Sentinel LDK Envelope

Sentinel LDK Envelope has been modified as described below:

- Script Envelope for Python applications (under Windows or Linux) now supports protecting model files for Pytorch and TensorFlow models.
- Sentinel LDK Envelope Now Builds a Protected Runtime and LDK Licensing API.

  The V3 protection engine used in Sentinel LDK Envelope for Windows now contains a dynamic runtime that embeds a secured version of Sentinel LDK Licensing API. As a result, the security of the licensing check at runtime has been significantly enhanced.

  > **NOTE** The first time that a developer performs the protection process for a given Batch Code on their machine, the new dynamic runtime is compiled from bitcode. This procedure adds 2 to 4 minutes to the protection process. Once compiled, the dynamic runtime is cached on the developer's machine. The compilation process is only repeated once for each Batch code and for each new version of Sentinel LDK Envelope.

- The V3 protection engine used in Sentinel LDK Envelope for Windows now supports **Periodic Background Checks** and **Allow grace period after failed checks**.
- When using Java method-level protection and background checks, Envelope now supports JDK 20 and JDK 21.
- Sentinel LDK Envelope now supports protecting applications for .NET 9.

Release: **10.0**

Enhancement to the VMType3 Clone Protection Scheme

The VMType3 clone protection scheme is now supported for the SL User Mode enforcement type for Linux platforms.

Windows Shell-Protection Support for DLL Assemblies

The V3 protection engine for Sentinel LDK Envelope has been enhanced as follows for .NET applications:

- For DLLs: DLL assemblies are now protected using the Windows shell-protection feature.
- For EXEs: The existing DFP-based Windows shell-protection continues to be used. This method can work for .NET Framework and .NET Core asse[illegible]s. The assemblies which have been protected using this feature will only work under Windows. The existing DFP-based protection will be used for EXE files.

Sentinel LDK Envelope Creates OMAP Files for Use with LDK Exception Report Translator

Envelope has been enhanced for using method-level protection for Java applications. You can now use the symbol obfuscation feature, but are still able to translate exception reports to a readable form that can help to analyze a crash.

Envelope now creates an OMAP file that contains the original and obfuscated names. The ERT (Exception Report Translator) tool is able to load the OMAP and display an exception trace with the original method names.

Enhanced Envelope Protection for Python Applications Under Linux

Script Envelope, which was recently released to protect Python applications under Windows, is now available for applying Sentinel LDK Envelope protection to Python applications on a Linux machine.

After you create a project file that contains protection parameters, you can protect the Python application simply by executing Script Envelope. No additional steps are required.

For details, see Sentinel LDK Envelope for Linux.

Enhancements to the LoginScope Function in Sentinel Licensing API

The LoginScope function in Sentinel Licensing API now provides more granular filtering capabilities for logging in to licenses. The Features that are accessed by LoginScope can be restricted to any of the following:

- A cloud license.
- A license that is detached or auto-detached from a cloud license.
- A non-cloud network license.

The GetInfo function can return attributes that differentiate between these license types.

In addition, the LoginScope function can specify that login should be limited to:

- A cloud license with specific Key ID.
- A license that is detached from a cloud license with a specific Key ID. (Users typically have multiple auto-detached keys from different CL keys.)
- A cloud license with a specific *family* (that is, a parent license with a specific Key ID or a license detached from that parent).

If a required detached license is not present, the LoginScope function can detach the required license if certain conditions are satisfied. For details, see Sentinel Licensing API C Reference.

Added Support for HTTPS Protocol

Communication between Licensing API or local license manager to vendor-hosted CL service or Thales-hosted CL service is now supporting using the HTTPS protocol.

Additional Enhancements/Changes to Sentinel LDK Envelope

Sentinel LDK Envelope has been modified as described below.

Enhancement for Java Applications

The number of classes/methods that can be protected in a Java application has been significantly increased.

Sentinel HL v.1.x Is No Longer Supported

Support for HL v.1.x has been discontinued. To protect an application that is licensed using HL v.1.x, use Sentinel LDK 9.0 or earlier.