Sentinel LDK 10.0

CHOOSING AND INTEGRATING HARDWARE-, SOFTWARE-, AND CLOUD LICENSING

Revision History

Document Number LE Revision A, 2306-1

Disclaimer and Copyrights

CONTENTS

Preface

Sentinel LDK supports several different methods for licensing software applications and software embedded in hardware devices:

> Sentinel HL (hardware-based) keys

> Sentinel SL (software-based) keys

> Sentinel CL (cloud licensing – an extension of Sentinel SL keys)

Many software vendor are familiar with only Sentinel HL keys and may be reluctant to consider using Sentinel SL licensing. The purpose of this guide is to provide a comparison between HL and SL licensing and provide an introduction to working with Sentinel SL key and cloud licensing.

The following topics are discussed:

Functional Differences Between HL, SL, and CL

This section describes the differences in functionality and benefits that are provided by HL (hardware licensing), SL (software licensing), and CL (SL with cloud licensing).

License Activation by User

HL	The licenses on HL keys are available for immediate use. Once the HL key is connected to a machine, the protected application can be run. No Internet connection is required.
SL	For online activation, requires Internet connection. For offline activation, requires exchange of files by email
CL	No activation required on the user machine

License Delivery

HL	Requires delivery of a physical HL key, with possible delays due to customs issues.
SL	A product key for activating the license for a protected application can be delivered immediately to the customer by email or other means. Once the customer receives the product key, they can activate the license for the application online in a matter of seconds.
CL	An identity string for running the protected application can be delivered immediately to the end user by email or other means.

Rehosting

HL	An HL license can be moved to a different machine simply by reconnecting the HL key to the required target machine.
SL	An SL license can be rehosted using the RUS tool (customized using Sentinel LDK-EMS) or calls to the Sentinel Licensing API.
CL	Rehosting keys from one machine to another is normally not needed with cloud licensing. Users can use the license from any internet-connected machine by simply installing the identity string.

AppOnChip Protection

HL	AppOnChip provide a very high level of protection against reverse-engineering of your application.
SL	Not available
CL	Not available

Dynamic Memory

HL	Provides expanded memory and ease-of-use.
SL	Supported.
CL	Supported.

Real-Time Clock

HL	The HL Time key and HL NetTime key provide a tamper-proof real-time clock. Regular HID keys provide the V-Clock (a virtual clock). **Note:** V-Clock does not provide the same level of control as the real-time clock in HL Time keys and HL NetTime keys. However, V-Clock prevents the end user from setting the system time back to an earlier date and time.
SL	SL keys provide the V-Clock (a virtual clock).
CL	Cloud-enabled SL keys provide the V-Clock (a virtual clock). If detach is not enabled, the time source remains the remote vendor-hosted server, where the system clock is not exposed to user tampering.

microSD Storage

HL	Both your software and the license can be stored on a Sentinel HL Drive microSD key, providing maximum mobility. The Sentinel HL Drive key contains up to 64 GB of flash memory on a microSD card in addition to the license data memory, enabling all of your software to reside on the key. This method is applicable for software that can be run from an external key without necessitating installation on a hard disk.
SL	Not available.
CL	Not available.

Network License Detaching

HL	Not available.
SL	While both HL and SL licenses support network seats (concurrency), only SL licenses support detaching a network seat from a license. This enables a user to temporarily move a license from their company network to their local machine. This is useful, for example, if the user wants to work with the protected application offline or if the network connection is unreliable.
CL	Cloud-enabled SL licenses support detaching multiple network seats from a license. This enables customers to set up second-level license servers in their networks.

Tamper Protection (Key Disabling)

HL	Your protected application can be configured to automatically disable the HL key used for licensing in the event that attempted tampering with the key is detected. This provides an additional layer of protection by discouraging attempts to bypass the licensing and protection for the application.
SL	Not available.
CL	Key disabling is available.

Additional Security Considerations

HL	The protection provided by Envelope can be enhanced by the use of AppOnChip to further encrypt the most mission-critical algorithms in your applications.
SL	The current generation of Sentinel SL key provide significant security against the misuse of protected applications.
CL	Cloud licensing provides an added level of protection for SL keys by enabling you to retain the SL keys within your own license server and, thus, out of the reach of any software crackers.

Benefits of Cloud Licensing

Sentinel LDK provides an alternative for SL-based licensing called cloud licensing. This model is based on software-based protection keys, but it provides an extension to the traditional model. The cloud licensing model provides a simpler mechanism, both for you (the vendor) and for the end user, for distributing and managing licenses.

Using this licensing model, you generate an SL key that supports cloud licensing for each customer organization. The SL key is installed on a license server machine (with Internet access) that is controlled by you. You install an SL license with concurrency for each application that the customer is authorized to use.

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

Cloud licensing provides the following benefits:

> **No need for end user to activate licenses**

   Each end user receives a unique "client identity" that they install on their machine. Once they install the client identity, they can immediately start to use the protected application. There is no requirement to activate a license or submit a device fingerprint to you.

> **Real-Time control over client identities**

   You can immediately deploy licenses to a cloud-based license server. They can issue and distribute client identitiesto end users or to the customers' organizations for distribution to end users. Creation or disabling of client identities are effective immediately.

> **Support of any cloud environment**

   You can deploy their license servers to any cloud infrastructure, such as AWS, MS Azure, GCP, AliCloud, or their own cloud infrastructure.

   Users can easily switch between machines without the manual steps involved with detaching an SL key.

> **High security**

   Cloud licensing provides a high level of security because the SL license is hosted on your license server (either in-house or in a cloud environment controlled by you), out of the reach of crackers.

   Client application can run in a VM, Docker, or on users' machines, and consume the remote cloud license. There is no way for users to change the license (since the license is hosted on a server that software crackers cannot access) or to benefit from spoofing their client VM identifiers.

   Cloud license provides secure licensing for applications hosted in VMs by untrusted customers. Users can spoof VM identifiers, but these are not used to lock the license (which is consumed from a remote cloud server).

   In contrast, if an SL license is hosted by the customer, they can revert the machine to a previous state or, in the case of VMs, they can spoof identifiers.

> **Cloud licensing server hosted by Thales**

   Thales offers a solution called Sentinel LDK CL Service. This is a hosted cloud licensing service for vendors who use Sentinel LDK and who subscribe to Sentinel EMS. When you subscribe to Sentinel LDK CL Service, Thales provides a high-availability license manager to serve cloud licenses to your customers, thus facilitating uninterrupted access to the cloud licenses that you push to the server.

> **Multi-level license servers**

   Cloud licensing gives you the option of allowing customers to set up a second level of license servers to provide greater control over the distribution of network seats within an organization and to minimize the overhead of license administration.

Changes to Workflow

This section summarizes the differences to the end users' experience when working with SL keys rather than HL keys.

> **NOTE** Unless indicated otherwise, the steps in the workflows in this section are performed by the customer.

Initial Use

This topic compares the user experience for initial use of the protected application when working with HL licensing, SL licensing, and Cloud licensing.

In all cases, it is assumed that the protected application and the Run-time Environment (when required) are installed on the end user's machine. For network licenses, the Run-time Environment is installed on the license server machine.

HL Licensing

Time required: Less than 1 minute.

Receive delivery of the HL key from the vendor. Attach the HL key to the end user's machine or (for network licenses) to the license server machine.

SL Licensing - Online Activation

Time required: Less than 1 minute.

1. Receive the product key from the vendor by email.

2. On the end user's machine or (for network licenses) the license server machine, click the link in the email to access the Sentinel LDK-EMS Customer Portal.

3. Paste the product key from the email into the Customer Portal.

> **NOTE** If the software is being supplied in a physical package, you can include a product key in the package. The user can type in the product key to log in to the Customer Portal.

4. On the Customer Portal web page, click **Online activation**.

SL Licensing - Offline Activation Using Sentinel LDK-EMS

Time required: Less than 5 minutes.

1. Receive the product key from the vendor by email.

2. On the end user's machine or (for network licenses) the license server machine, use the Admin Control Center or other tool to create a C2V file containing a fingerprint of the machine. Transfer the C2V file to a machine with Internet access.

3. On the Internet machine, use the product key to log in to the Sentinel LDK-EMS Customer Portal.

   > **NOTE** If the software is being supplied in a physical package, you can include a product key in the package. The user can type in the product key to log in to the Customer Portal.

4. Click **Offline activation**. Upload the C2V file.

5. Download a generated V2C file. Transfer the V2C file to the target machine.

6. On the target machine, use the Admin Control Center or other tool to apply the V2C file.

SL Licensing - Offline Activation Using Sentinel LDK License Generation API

Time required: Depends on your response time.

1. On the end user's machine or (for network licenses) the license server machine, use the Admin Control Center or other tool to create a C2V file containing a fingerprint of the machine. Transfer the C2V file to a machine with Internet access.

2. Send the C2V file to the vendor by email or other means.

   The vendor uses Sentinel License Generation API to generate a V2C file containing a license to use the protected application. The following API functions are used:

   a. **sntl_lg_initialize**

   b. **sntl_lg_start** using license type SNTL_LG_LICENSE_TYPE_UPDATE.

   c. **sntl_lg_generate_license** – Save the generated V2C file.

   d. **sntl_lg_cleanup**

   For an example of this procedure, see "Lesson 6: Creating and Distributing a Sentinel SL-protected Software Order" in the Sentinel LDK Software Protection and Licensing API Tutorial (Starter Kit).

   The vendor returns the V2C file to the customer by email.

3. Receive the generated V2C file and transfer it to the target machine.

4. On the target machine, use the Admin Control Center or other tool to apply the V2C file.

SL Licensing - Online Activation Using Sentinel LDK-EMS and 3rd Party Software

Time required: Activation is instantaneous.

Vendors can use a combination of marketplace software and Sentinel LDK-EMS web services to handle receipt of payment and automatic activation of the protected applications.

Cloud Licensing (Connected mode)

Time required: Less than 5 minutes.

1. Each end user receives a personalized client identity string by email.

2. The end user installs their identity string on their machine (or on multiple machines if allowed) using one of the following methods:

   - In Admin Control Center, go to **Configuration > Access to Remote License Managers** tab. Enter the identity string in **Remote License Search Parameters**.

   - Manually add the identity string to the local License Manager configuration file.

   These operations can also be performed programmatically.

Cloud Licensing (Detached mode)

Time required: Activation is instantaneous for the end users.

Using Admin Control Center, an administrator in the customer organization detaches an SL license with concurrency from the vendor's license server to one or more second-level license servers. The administrator configures the License Manager to indicate which end users can access network seats for the detached license.

Authorized end users can access network seats with no action required on their part.

Portability

This topic compares the user experience for moving the license to a different machine when working with HL licensing, SL licensing, and Cloud licensing.

In all cases, it is assumed that the protected application and the Run-time Environment (when required) are installed on the target machine.

HL Licensing

Time required: Less than 1 minute.

Disconnect the HL key from the current machine. Attach the HL key to the target machine.

SL Licensing

Time required: 2-5 minutes.

1. On the target machine, use the RUS utility or Licensing API to collect information about the machine and save it to a file.

2. On the source machine, use the RUS utility or Licensing API to read the file from step 1 and to generate the license transfer H2H file.

3. On the target machine, use the RUS utility or Licensing API to apply the license transfer H2H file from step 2.

Cloud Licensing (Connected Mode)

Time required: Less than 5 minute.

If your client identity supports multiple machines, install your identity string on the target machine as described earlier.

If you have already installed your identity string on the maximum number of machines allowed to you:

1. Ask the cloud licenses administrator to unregister one of your machines or to increase the maximum number of allowed machines for your client identity.

2. Install your identity string on the target machine.

Cloud Licensing (Detached Mode)

Time required: Activation is instantaneous for the end users.

You can use the protected application wherever you are logged in within the LAN.

Updating the Sentinel LDK-EMS Catalog

Using HL Keys for Licensing

When you create a Product in the Sentinel LDK-EMS catalog, the Product is assigned the locking type **HL**. As a result, the Product can only be licensing using HL keys.

Vendors who planned to use only HL keys for licensing most likely accepted the default locking type. As a result, they cannot issue SL keys to license the Product.

> **NOTE** Starting with Sentinel LDK 8.4, the default locking type for new Products will be **HL or SL (AdminMode or UserMode)**. Vendors who accept the default locking type when defining new Products in Sentinel LDK 8.4 or later will be able to use either HL key or SL keys to distribute licenses for their protected applications.

Using SL Keys for Licensing

To enable the use of SL keys when your Products have been defined with the **HL** locking type, do the following:

> For Sentinel LDK 8.4 and later:
>
> You can change the locking type of existing Products in the Catalog to **HL or SL (AdminMode or UserMode**. There is no need to create new Products.

> For Sentinel LDK 8.3 and earlier:
>
> a. In the **Catalog** tab, create copies of the relevant Products.
>
> b. In each copied Product, assign the locking type **HL or SL (AdminMode or UserMode**.
>
> Use the new Products when fulfilling orders for new customers.

Using Cloud Licensing

To use cloud licensing to license your applications, you set up your own license server machine and install an SL key for each customer organization. You provide client identities for each end user or you enable the customer organization to set up second-level license servers to provide licenses for the end users.

When you use Sentinel LDK-EMS to create or update the SL keys, ensure that the Sentinel LDK-EMS configuration parameter **Cloud Licensing** is enabled.

Generating Entitlements

This section describes the differences in generating entitlements for HL licensing, SL licensing, and cloud licensing

For HL Licenses

To generate an entitlement for an HL license:

1. The vendor selects the entitlement type **Hardware key**.

2. The vendor selects a Product that includes the locking type **HL** and then clicks **Burn** to burn the license to the connected HL key.

To generate an update to an existing HL license:

1. The vendor selects the entitlement type **Protection Key Update**

2. The vendor selects the relevant product and then clicks **Update** to generate an update to the existing HL key.

3. Sentinel LDK-EMS generates an email to deliver the protection key update to the customer.

4. The customer applies the update to the HL key using the Sentinel LDK-EMS Customer Portal.

For SL Licenses

To generate an entitlement for an SL license:

1. The vendor selects the entitlement type **Product Key**.

2. The vendor selects a Product that includes the locking type **SL** and then clicks **Produce** to generate a product key.

3. Sentinel LDK-EMS generates an email to deliver the product key to the customer.

4. The customer uses the product key to log in to Sentinel LDK-EMS Customer Portal update and install the SL key on the license server machine or end user machine.

To generate an update to an existing SL key:

1. The vendor selects the entitlement type **Protection Key Update**

2. The vendor selects the relevant product and then clicks **Update** to generate an update to the existing SL key.

3. Sentinel LDK-EMS generates an email to deliver the protection key update to the customer.

4. The customer applies the update to the SL key using the Sentinel LDK-EMS Customer Portal.

> **NOTE** The update procedure above can also be used to generate a new SL key instead of using a product key.

For Cloud Licenses

The vendor generates an entitlement that automatically creates and installs a cloud-enabled SL key on their license server in a single operation using the **Produce & Push** option in the Entitlement screen.

After creating the cloud-enabled SL key on the license server machine, the vendor can generate client identities and provide identity strings for end users or allow the customer to detach licenses from the cloud-enabled SL key for second-level license servers at the customer's sites.

Client identities are generated using Admin Control Center (described in Sentinel LDK Software Protection and Licensing Guide) or using Sentinel Admin API (see "Managing Client Identities of Cloud Licenses " on page 18).

Automating License Generation for SL Keys

Generating and distributing SL keys requires more steps than generation HL keys. This section describes how you can use back-end automation to generate licenses for SL keys.

Sentinel LDK automation tools consist of one of the following

> Sentinel License Generation API

> Sentinel EMS Rest API or Sentinel LDK-EMS Web Services

Either tool can be integrated with your back end system.

Handling SL Keys with Sentinel License Generation API

To generate an SL license for a protected application using the Sentinel License Generation API, your back-end needs to handle the following functions:

> Define Features

> Define Products

> Define customers

> Handle customer orders

The back-end and the protected application can use Sentinel APIs to generate and install an SL license as follows:

1. Obtain a fingerprint of the target machine from the customer.

   Several methods are available to accomplish this. A common method is to include a routine in the protected application to call the **GetInfo** function in the Sentinel Licensing API. The **GetInfo** function can use the HASP_FINGERPRINTpredefined alias to retrieve the fingerprint of the machine where the application is installed and write the fingerprint to a C2V file.

2. Send the C2V file to the vendor via email (or other methods).

3. At the vendor's site, use Sentinel License Generation API to generate the SL license:

   a. Call **sntl_lg_initialize**

   b. Call **sntl_lg_start**. Use the license type SNTL_LG_LICENSE_TYPE_UPDATE. For current state, use the C2V file received from the customer.

   c. Call **sntl_lg_generate_license**. Save the generated license to a V2C file.

4. Send the V2C file to the customer via email.

5. On the target machine, call the **Update** function in the Sentinel Licensing API to apply the V2C file and write the license to an SL key.

For more information see Sentinel Licensing API Reference and Sentinel License Generation API Reference.

Handling SL Keys with Sentinel Web Services

When working with SL keys, there is a significant advantage to handling license generation and delivery using Sentinel LDK-EMS web services.

Sentinel LDK-EMS provides a database for managing products, features, protection keys. and entitlements. This functionality can be integrated in your back end using web services.

Sentinel LDK-EMS also allows the vendor to generate product keys for entitlements. The use of product keys greatly simplifies the process of activating an SL license on an end user's machine or on a license server machine.

Your back-end system can call web services to:

> Define Features

> Define Products

> Define customers

> Handle entitlements

   The web service that generates entitlements can

   a. Define the entitlement

   b. Generate a product key for the entitlement

   c. Generate an email to deliver the entitlement to the customer. The entitlement can contain one or more product keys, each of which can be used to install one or more SL keys on end users' machines or on license server machines.

Each end user click a provided link to access the Sentinel LDK-EMS Customer Portal. The user logs in to the Portal using the product key and clicks a link to activate an SL license on their machine. The Customer Portal automatically performs the necessary step to:

a. Obtain a fingerprint of the user's machine.

b. Install and activate a the license in an SL key on the user's machine.

Using a product key, the process of obtaining a fingerprint and activating the SL license on the target machine can be accomplished in a matter of seconds.

For more information, see Sentinel LDK–EMS Web Services Guide

Managing Client Identities of Cloud Licenses

Generation and management of client identities for cloud licenses can be handled using Sentinel Admin API. Your back end can call the **get** and **set** functions in Admin API to perform the following actions:

> Retrieve a single client identity

> Read a client identity list

> Create a client identity

> Enable or disable a client identity

> Update a client identity

> Delete a client identity.

For more information, see Sentinel Admin API Reference.

Master License Requirements

This section describes the modules that you require in your Sentinel LDK Master license in order to work with SL licensing and cloud licensing.

For additional details, see Sentinel LDK Software Protection and Licensing Guide.

Required Modules for SL Licensing

To work with SL licenses, you required the following modules in your Sentinel LDK Master license:

> **New SL Key Pool**

Required for generating new SL keys. Each time a new SL key is created for a given machine at a customer site, an SL key unit is consumed from this pool.

You can either purchase a quantity of SL keys for the pool, or you can subscribe to receive an unlimited number of SL keys.

> **SL Pool of Seats**

Required for providing network seats in an SL license. Each time a customer activates your software, the number of concurrent instances that you included in the Product is deducted from the SL Pool of Seats on your Sentinel LDK Master license.

You can either purchase a quantity of network seats for the pool, or you can subscribe to receive an unlimited number of network seats.

> **Product Activation module (optional)**

Sentinel LDK provides a mechanism to easily perform interactive license updates on an end user's machine. This is accomplished by generating a Product Key for an entitlement in Sentinel LDK-EMS and providing this code to the end user. The end user accesses theSentinel LDK-EMS Customer Portal over the Internet and enters the Product Key. Sentinel LDK-EMS then retrieves the necessary information about the end user's machine or existing license and completes the process to update the license on the user's machine. (This process can also be accomplished in program code using Sentinel LDK-EMS Web Services.)

You purchase a subscription for the Product Activation module for a defined period of time.

The Product Activation module is not required if you only want to use the Product Key mechanism to update HL keys.

Required Modules for Cloud Licensing

To work with Cloud licenses, you require all of the modules described above for SL licensing. In addition, you required the following module:

> **Cloud Licensing module**

   To generate and update SL licenses that grant license access based on identity strings, your Sentinel LDK Master license must contain the Cloud Licensing module.