THALES

Sentinel LDK 8.0 Patch 12/2020: EMS and Vendor Suite (KB0023249)

RELEASE NOTES

Issue Date: 27 December 2020

Contents

Release Overview

This document describes the release of Sentinel LDK 8.0 Patch 12/2020: EMS and Vendor Suite (KB0023249).

Note the following:

> This patch includes all the enhancements and corrections that were include in Patch 8/2020 and in Patch 10/2020 as well as a number of new enhancements and corrections.

> You must install Run-time Environment version 8.15 on all vendor and customer machines in order to support all new functionality provided by this patch.

> *This release enhances the security of the Run-time Environment. Thales highly recommends that you install this release to ensure maximum security for your protected applications.*

> You must download the latest vendor libraries using Sentinel Master Wizard before protecting your applications with Sentinel LDK Envelope or Sentinel Licensing API.

Installing the Patch

The Software Manager for Sentinel LDK will deliver this patch to vendors who are currently using Sentinel LDK 8.0.1. The patch will be delivered to each Windows machine that is online and on which Sentinel Vendor Suite or Sentinel EMS is installed.

To install the patch:

1. Click the **Install** button in the notification screen that is automatically displayed on the Windows machine where Sentinel LDK is installed. The updated product components and documentation are automatically installed.

2. In Sentinel EMS Vendor Portal, click **Administration > Administration Console**. In the Administration Console, click **Generate/Update Lucene Search Index** at the bottom of the page.

New Features and Enhancements

This release includes the enhancements described below.

Automatic Detach for Licenses

Sentinel LDK Run-time Environment now supports a new method for detaching licenses, referred to as *Automatic Detach*.

When Automatic Detach is enabled, a protected application automatically detaches a network seat from an SL key (that supports concurrency) when the application requires a license. As a result, the application can continue to operate even if the connection to the SL key is interrupted. The application retains the license for a predefined number of hours.

This method is especially useful when working with cloud licenses.

For details, see the description of detaching licenses in the Admin Control Center help system.

Sentinel EMS User Interface Customization

You can now configure the look and feel of Sentinel EMS Vendor Portal and Customer Portal with your own logo, favicon and color scheme. This lets you expand your brand identity to improve user experience. Only a user with administrative rights can view and access the UI Branding section in the Administration Console. For details, see Sentinel EMS User Guide.

Simplified SL Key Creation and Updates in Sentinel EMS for Vendor-hosted Cloud Licenses

You can now use Sentinel EMS to produce an entitlement and push it to your cloud license server in a single operation.

When you create an entitlement, you can click **Produce & Push** to produce the entitlement and push the SL key or license update to your cloud license server machine. This simplifies the process and removes several steps which otherwise need to be performed manually. For a Product Key, clicking **Produce & Push** results in a new SL key on the license server. For a Protection Key update for a single key, this updates the selected key on the license server. For details, see Sentinel EMS User Guide.

Strong Password Policy for Logging in to Sentinel EMS

You can now require strong passwords for users that log in via Sentinel EMS Vendor Portal or a Web Service. This applies both for new and existing users. Passwords must meet the following criteria:

> 8 to 30 characters long

> At least one uppercase letter (A-Z) and one lowercase letter (a-z)

> At least one number (0-9) or special character (! @ # $ % ^ & * ( ) _ - + = , .)

For new installations, this policy is applied by default.

When upgrading from an earlier version, the setting for this policy remains unchecked to maintain seamless access. You can apply the strong password policy if needed. For details, see Sentinel EMS Configuration Guide.

Strong Password Policy for Logging in to the Admin License Manager

When setting or changing the password for accessing Sentinel Admin License Manager (using Admin Control Center or Sentinel Admin API), you must now specify a strong password. The password must satisfy the following requirements:

> At least eight characters long

> At least one uppercase letter (A-Z) and one lowercase letter (a-z)

> At least one number (0-9) or special character (for example: ! @ # $ % ^ & * " ( ) . , - +)

These requirements are enforced when a password is added or changed. There is no warning or action required if the existing password does not satisfy these requirements.

Defining Password for Sentinel EMS Users

Sentinel EMS users can now set their own password.

When you create a user, you can now either specify the user's password yourself or generate an email asking the user to set their password. For details, see Sentinel EMS User Guide.

Custom Clone Protection Scheme Enhancement

For increased security, you can now require a license to meet all of the clone protection criteria that matched when the license was generated.

Each custom clone protection scheme contains the **Minimum Required Criteria** parameter that states how many of the selected identifiers must be met for the license to be validated. For stronger protection against cloning, you can select the option **All identifiers present at license generation must exist and match at runtime**. When selected, all of the identifiers that were selected and were present when the license was generated must exist and match when the license is validated to run the protected application.

For example, suppose the **Minimum Required Criteria** in your custom clone protection scheme requires 4 out of 5 criteria in the fingerprint. If this new option is selected, and all 5 of the criteria were present when the license was generated, then all 5 of the criteria must match the fingerprint at runtime, even though the custom clone protection scheme requires only 4.

For details, see Sentinel EMS User Guide.

Detached Licenses Now Use the "Platform Default" Clone Protection Scheme

When a license is detached from an SL key on a license server, the detached license is now assigned the **Platform Default** clone protection scheme. This ensures that the detached license is protected with the most appropriate clone protection scheme for the platform where the license will be attached.

> **NOTE** The **Platform Default** scheme is assigned regardless of whether clone protection was enabled for the Product license on the license server from which the license was detached.

For details, see Sentinel EMS User Guide.

Enhancements to Sentinel LDK Envelope

Electron Support
Envelope for Windows has been enhanced to support Electron applications.

Extended Support for .NET
Applications protected using Sentinel LDK Envelope now support the .NET v5.0 framework.

Improvement to Envelope User Interface for .NET and Java Applications
When the **Feature ID** is set to Default (0), Envelope now sets the parameter **Frequency** to **Once per program** and disables the setting to define frequency for method-level protection. This blocks the user from accidentally defining an invalid request. (If checking the protection key is already defined to be performed once, then defining the frequency of checks is not applicable.)

Support for Oracle Java 11 and Open JDK 14
Sentinel LDK Envelope under Windows now supports the protection of Oracle JDK 11 and Open JDK 14 applications for Windows, Linux, and Mac. This includes applications that use the Java Platform Module System (JPMS).

As part of the protection process, Envelope generates files that contain the command required to execute module-based applications on different platforms. You must modify these files before using them to execute the protected application.

For details, see the help system for Sentinel LDK Envelope.

Updated External License Manager

External License Manager version 24.4 is included in this patch. This provides optimal compatibility with the customized Vendor Library version 8.15 that you can download using the Master Wizard.

Stronger Security for Admin License Manager Configuration

When you enable remote access to Admin Control Center, you must now enable password protection for accessing the configuration pages for Admin Control Center. You have the option of requiring a password to access *any* part of Admin Control Center

Cloud Licensing Supports Multiple Key IDs for Client Identities

When creating a client identity for cloud licensing and specifying the **Limit to Key ID** parameter in Admin Control Center (or Admin API), you can now specify multiple key IDs for a given client identity.

Domain Name Can Now Be Used to Restrict User Access to a License Server Machine

Admin Control Center enables a customer to specify which users can access a license on a license server machine.

You can now include domain names as part of the restrictions that they specify for this purpose. For example, you can now specify:

```
allow=username@hostname.domainname,...
allow=khsingh@noi-2n39623.thalesgroup.com
```

For details, see the description of the **User Restrictions** parameter on the **Configuration > Users** page of Admin Control Center.

Admin License Manager Can Now Listen on Port 80

Network licenses will be accessible even if port 1947 is not open in the firewall. To enable this enhancement, you must select the option **Listen for clients also on port 80** in the Admin Control Center configuration.

Reduced Installation Time for Run-time Environment

(Windows only) If the installed Run-time Environment is version 7.101 or later, it is no longer uninstalled before installing the new Run-time Environment. (This is because the driver binary has not been updated in the new version.) As a result, the installation time for the new Run-time Environment will be reduced if the same version of the driver binary is already installed in the system.

Enhanced Support for VMType3

(This enhancement was included in Sentinel LDK Patch 8/2020)

Clone protection scheme **VMType3**, intended for cloud computing services, now supports Amazon EC2 in addition to Microsoft Azure. This provides enhanced clone protection for protected applications that execute on these platforms.

Sentinel License Generation API has been updated to support the enhancements for **VMType3**. The patch installs the updated version of Sentinel License Generation API on each machine where Sentinel Vendor Suite or Sentinel EMS is present.

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

Support for Cloud Licensing in Sentinel Admin API and ToolBox

(This enhancement was included in Sentinel LDK Patch 8/2020)

Sentinel Admin API now contains functionality to support operations for cloud licensing. This enables you or your customers to automate actions required to implement and maintain cloud licenses.

The following operations are supported:

> Retrieve a single client identity

> Retrieve a list of client identities

> Create a client identity

> Update or disable a client identity

> Delete a client identity

> Unregister a machine

Sentinel LDK ToolBox has been enhanced to support these enhancements in Sentinel Admin API.

Enhancements to Sentinel LDK Envelope

(This enhancement was included in Sentinel LDK Patch 8/2020)

Sentinel LDK Envelope provides support for the two official "long term support" versions of .NET Core framework (V2.1 and 3.1).

Envelope also supports protected applications to run on Linux x64, ARMHF and ARM64 platforms.

.NET Core applications with platform-specific functionality such as Windows Forms and Windows Presentation Foundation (WPF) work only on Windows platforms.

For details, see **.NET Core Version and Platform Support** in the Sentinel LDK Envelope help system.

Changes to Documentation

Documentation for Cloud Licensing Performance Has Been Improved

The description of performance considerations for cloud licensing has been improved in the online version of Sentinel LDK Software Protection and Licensing Guide.

Run-time Environment Readme Documentation is Now in HTML5 Format

The documentation for each variation of Run-time Environment (RTE) is now provided in HTML5 format. As a result, the documentation is modular and easier to navigate.

Because of this change, the path for accessing the documents online has changed. If you created shortcuts to access RTE documentation from the Thales web site, you must modify your shortcuts accordingly.

The paths for accessing the online RTE Readme files are available from: https://docs.sentinel.thalesgroup.com/ldk/rte.htm

Update to Sentinel LDK Documentation for haspdinst.exe

(This enhancement was included in Sentinel LDK Patch 8/2020)

Online documentation for Sentinel LDK 8.0 has been updated to document a change to the behavior of **haspdinst.exe**.

When the command `haspdinst.exe -i` is executed: Immediately after the Run-time Environment is installed or upgraded, any V2C file contained in the same folder is applied to the relevant protection key on the machine.

This change was introduced in Sentinel LDK 7.10. Sentinel LDK Run-time Environment 7.100 or later must be present on the machine for the change to take effect.

Documentation has been updated:

> in the online version of Sentinel LDK Installation Guide

> in the readme file for the Run-time Environment 8.13 Command-line Installer

This changes will be included in Sentinel LDK Installation Guide for Sentinel LDK 8.2.

Update to Documentation for Vendor Library Version Dependency

(This enhancement was included in Sentinel LDK Patch 10/2020)

The Sentinel LDK 8.0 Release Notes (online version) and Sentinel LDK Software Protection and Licensing Guide (online version and included in the Sentinel LDK installation) have been updated

> The Release Notes now include a section that describes the version dependencies between the customized vendor library and the Run-time Environment, and between the customized vendor library and the External License Manager. For details, see *Sentinel LDK Release Notes* – "Vendor Library Version Dependency".

> The Software Protection and Licensing Guide provides a link to the above section in the Release Notes from the relevant location. For details, see Software for SL Licenses in Sentinel LDK Software Protection and Licensing Guide.

Update to Sentinel LDK Envelope Documentation

(This enhancement was included in Sentinel LDK Patch 8/2020)

Documentation for Sentinel LDK Envelope has been updated to include information regarding the following advanced protection parameters for Windows applications:

> ADVANCED_DEBUGGER_DETECTION

> KEEP_DEBUG_INFO

> CONFIGURATION_STRING

Planned Changes for Sentinel LDK 8.2

The following changes are planned for Sentinel LDK 8.2:

> For new installation of Sentinel LDK-EMS:

- Windows 10 will be required. Sentinel LDK EMS will be installed with MSSQL 2019.

- Windows 7 is no longer supported. If you want to install Sentinel LDK-EMS on a Windows 7 machine, install version 8.0.

> For upgrades of Sentinel LDK-EMS: The installer will issue a warning that Windows 7 support will be removed in the next release because Microsoft no longer provides security updates for Windows 7.

Users will be provided with the option to quit the installation (to upgrade to Windows 10) or to continue with the already-installed MSSQL 2014.

Planned Drop of Support

Sentinel LDK Envelope for RTEXE and Internet Explorer plugin support life cycle is scheduled to change on the following dates:

> End-of-Development: 31-Dec-2020

> End-of-Support: 31-Dec-2021

For details on the Thales product life cycle process, see: https://supportportal.thalesgroup.com/csm?id=kb_restricted&sysparm_article=KB0022992

Issues Resolved

The following issues are resolved in this release.

Reference	Description	Component
SM-90271	Documentation for Sentinel License Generation API has been corrected as follows: > Placement of the <minimum_rte_api_version> tag has been moved from the Product level of the XML code to the protection key level. This parameter relates to all the Products in the protection key, not to a specific Product. > Documentation for the <rehost> tag has been updated to indicate that the <minimum_rte_api_version> tag (if used), must be placed before the <rehost> tag in the XML code.	Documentation
SM-77887	(Linux) SSH session was not detected if the customer runs an application using sudo or su.	Licensing API
SM-83674	Failed to call integrated Admin API without the vendor code.	Licensing API

Reference	Description	Component
SM-83787	(Linux) Login calls would fail on Linux ARM64 platform. Output was "Bus error".	Licensing API
SM-86082	(Linux) The upper limit for the number of sockets was too low, resulting in a login error in certain circumstances.	Licensing API
SM-82050	Android sample would fail on Android 11 emulator/real device.	Licensing API
SM-90482	Calling Web Service update protection key with action of ConvertV2CToExe would result in a memory leak.	Sentinel EMS
SM-73900	Login would fail with error code 500 while running the EMS web service demo.	Sentinel EMS
SM-78585	The status value of product key should not be changed if relevant entitlement is disabled.	Sentinel EMS
SM-89552	Descriptive text for warning 2044 has been provided.	Sentinel EMS
SM-90954	.NET Engine would fails when adding a sample with an excessively long class name.	Envelope
SM-90780	A .ctor issue with Envelope.Net was resolved.	Envelope
SM-88548	Envelope would crash when adding .NET App.	Envelope
SM-80748	The PE checksums for executables were calculated incorrectly after protection with Envelope.	Envelope
SM-82498	Under certain circumstances, the License Generation DLL would crash when generating a clearClone V2C.	License Generation API
SM-82026 SM-82827	Resolve a compatibility problem for PMType3 SL UserMode license definition.	License Generation API

The following issues were resolved in Patch 8/2020 and in Patch 10/2020 and are also resolved in this release.

Reference	Description
SM-79715	For the **VMType4** clone protection scheme, generating a **Clear Clone** license would use CPU_UID instead of CPU for the fingerprint.
SM-80400	On the Entitlements page in Sentinel EMS: When performing a search using **Customer Name** and then sorting the results by **Ref ID 2**, an internal error would occur.

Reference	Description
SM-80548	Under certain circumstances, when using Sentinel LDK Toolbox to generate a license update to enable Remote Desktop, the License Generation would fail with error 5009 ("License definition is invalid").
SM-80815	When using AppOnChip, Envelope would fail during startup on old Intel processor platforms (Atom/Core2).
SM-81865	When a debugger is in use, an application protected with AppOnChip would display the message **Debugger detected**. When the user dismissed the message box, the application would exit. Now, under the same circumstances, the message box displays a warning. The message can be dismissed without terminating the application.
SM-82167	Under certain circumstances, when CodeObfuscation is set to **True**, Envelope would fail when protecting an application.
SM-82260	Given the following circumstances: 1. In Sentinel EMS, copy an entitlement that has already been produced. 2. Add Products to the copied entitlement. The **Exclude All** button for Features was not accessible. Features had to be individually excluded from the Entitlement.
SM-83026	Sentinel LDK Envelope 8.0 would fail while adding or protecting a .NET Core file.
SM-83050	Given the following circumstances: > In Sentinel EMS Administration Console, Sentinel EMS is configured to generate V2C files using the customer name in the name of the V2C file. > The name of a customer in Sentinel EMS contains a comma (for example: **test, name**). > An entitlement is generated for the above customer. The resulting V2C file could not be downloaded.
SM-83309	When Sentinel EMS 8.0.1 is installed with Java 8 Update 261, Sentinel EMS would start correctly, but the login page was blank.
SM-86349	Applications protected with Envelope were not logging errors properly.
SM-86459	An issue in the External License Manager has been resolved