

License Activation User Guide

# Purpose

This document serves as a guide to show how to activate license in the Thales Sentinel User Portal. *(*[*https://gemaltocogentinc.prod.sentinelcloud.com/ems/customerLogin.html*](https://gemaltocogentinc.prod.sentinelcloud.com/ems/customerLogin.html)*)*

# Introduction

In order to use the Thales Algorithm API, you need to activate your license. After the activation, the license usage will be restricted to the hardware of the workstation on which the Algorithm API is installed.

Once you have received your user account there are a two ways to activate the SDK licenses depending on your network situation.

**Offline – Mode:**

The offline mode can be used for the cases where the workstation doesn’t have internet access.

**Online – Mode**

The online mode can be used for the cases where the workstation is connected to the

internet at the first authority time.

# Prerequisites

Before activating the licenses please verify that you have access to a computer connected to the Thales Sentinel User Portal and that you have local administrator rights to install the license on a specific workstation and be able to generate the Workstation locking code as described below.

Before Thales can create a license code you have to provide the locking code for your computer with the echoid program. Wechoid utility is the windows interface of echoid. echoid64/echoid utility is the linux interface of echoid(Wechoid,echoid64 and echoid are part of the SDK delivery package). The following points are important to understand the Wechoid interface.

**1.** When launched, the utility shows the available lock criteria (a checkmark will be placed next to them) and their values.

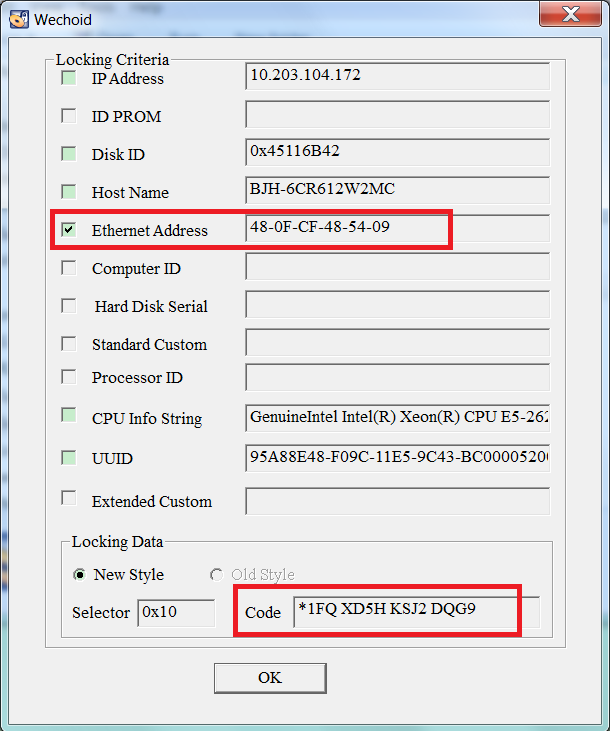
**2.** The unavailable locking criteria will be shown disabled.

**3.** The Computer ID will be enabled if a parallel/USB CID key is attached to your system.

**4.** The Standard Custom and/or Extended Custom will be enabled only if the software vendor has chosen them for you.

**NOTE**   The file *wechoid.exe.manifest* file must be in the current working directory from where the wechoid program file is run. This file defines what criteria will make up the fingerprint and is shipped along with the wechoid executable.

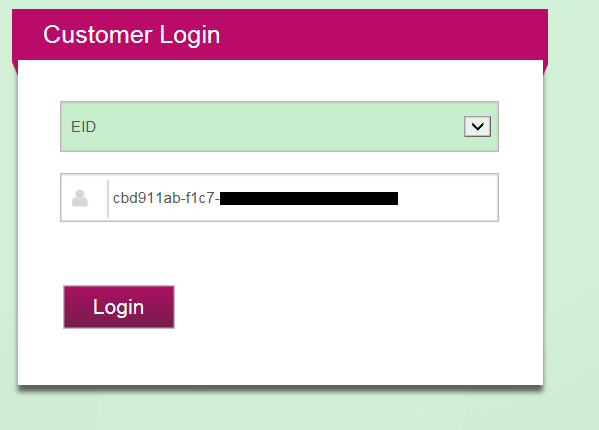
Please only enable the “Ethernet Address” as shown in the example below and copy the Code.



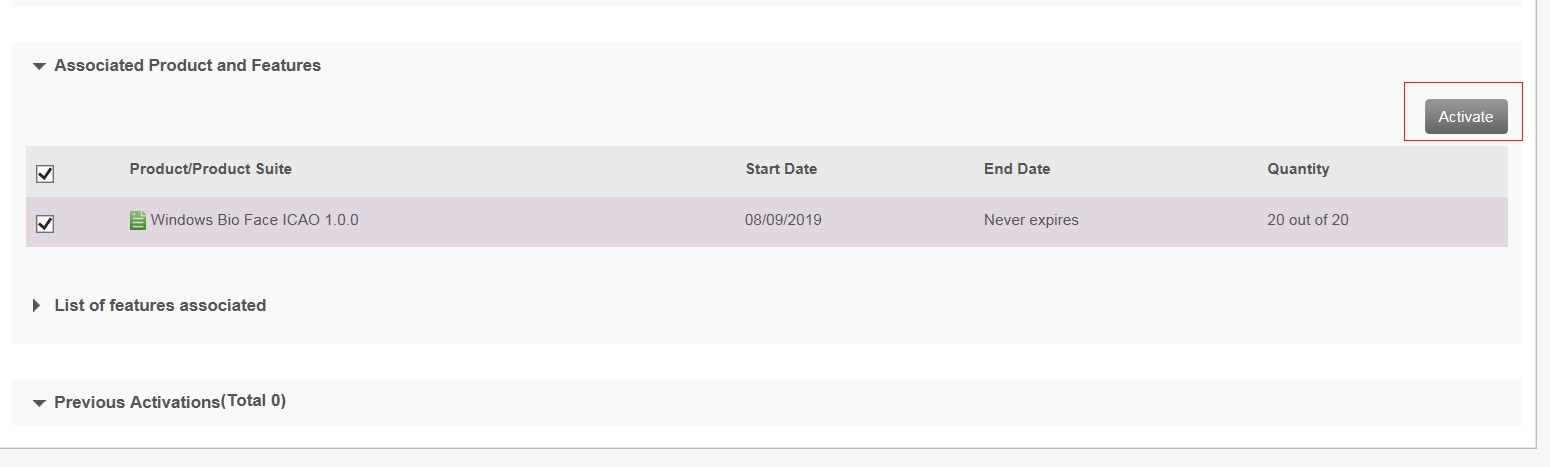
# License Activation (offline mode)

***Step 1***: Please log on to the Thales Sentinel User Portal (requires internet access)

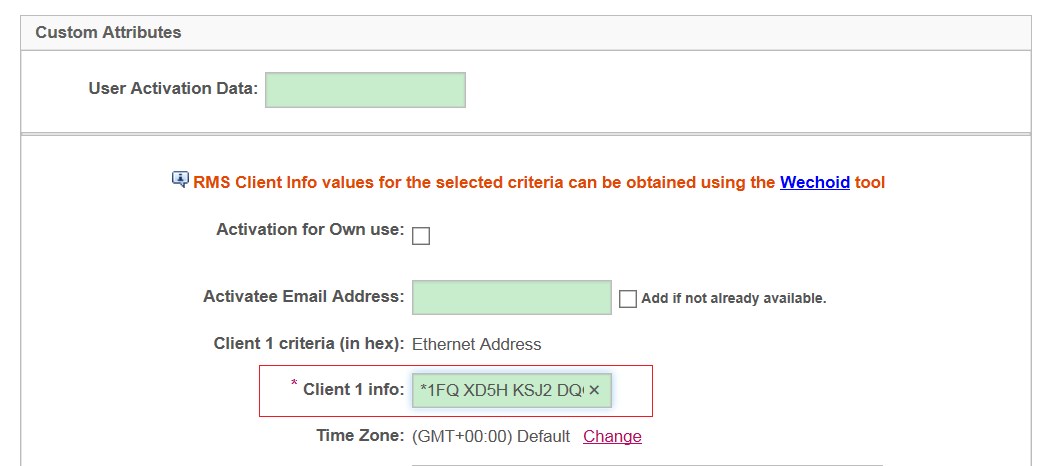
[*https://gemaltocogentinc.prod.sentinelcloud.com/ems/customerLogin.html*](https://gemaltocogentinc.prod.sentinelcloud.com/ems/customerLogin.html)



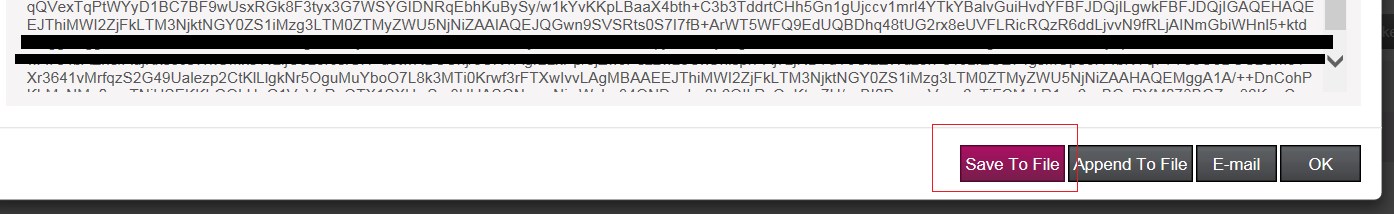
* 1. Input your EID or user information. The information will be sent to customer after buy the license.
  2. Click Register Later!
  3. You should be able to visualize all assigned licenses for your user account. Click Activate button.



***Step 2:***Please chose one license and enter the required Activation Data including the previously obtained Lock Code (see Pre-requisites). Then click “activate”.



***Step 3****:* Click save to file and save the name as***cgtbiosdkforrms.lic***



***Step 4***: please go to your user directory and create the CgtBioSDKforRMS directory*.*

*eg.C:\Users\10051876\CgtBioSDKforRMS*

***Step 5****:* Copy your downloaded license file to this directory.

***Windows****:*

*eg. C:\Users\10051876\CgtBioSDKforRMS*

***Linux:***

*Please save in the Env "HOME" value directory.*

*eg. /home/test/CgtBioSDKforRMS (please check the exact folder using cmd: echo $HOME)*

*Please note that the file of cacert.pem is needed for license verification. (cacert.pem is part of the SDK delivery package)*

*Please make sure to copy this file to the directory of CgtBioSDKforRMS in Linux OS.*

**Step 6**: Incorporate the following code in your application, please set the sentinel license get method as “Manually”

Eg. Algorithm BioAPI initialize:

*pnParamInit[19]= 1; //Manually*

*nRet = CgtBioAPI\_Initialize(pDataBuf, nDataSize, NULL,pnParamInit, pszMsg);*

Eg. Algorithm Fingerprint API initialize:

*pnParamInit[109]= 1; //Manually*

*nRet = CgtFinger\_Initialize (pDataBuf, nDataSize, NULL,pnParamInit, pszMsg);*

Eg. Algorithm Face API initialize:

*pnParamInit[109]= 1; //Manually*

*nRet = CgtFace\_Initialize\_Ex(pDataBuf, nDataSize, NULL,pnParamInit, pszMsg);*

# License Activation (online /cloud mode)

***Step 1****:* Please make sure the workstation is connected to the internet

***Step 2:***  Please go to your user directory and create the CgtBioSDKforRMS directory*.*

***Windows****:*

*eg. C:\Users\10051876\CgtBioSDKforRMS*

***Linux:***

*The RMS cloud config file will save in the Env "HOME" value directory.*

*eg. /home/test/CgtBioSDKforRMS (please check the exact folder using cmd: echo $HOME)*

*Please note that the file of cacert.pem is needed for license verification.*

*Please make sure to copy this file to the directory of CgtBioSDKforRMS in Linux OS.*

**Step 3**: Please incorporate the following code in your application:

*char ptrArry[16][256]={"422ad5c-43ec-46bd-9dff0-e026314892","BJH6CR612W2MC","http://proxy-sg-singapore.gemalto.com","","","8080"};*

*char \*pLicConfigPara[16];*

*for(int i=0;i<16;i++)*

*pLicConfigPara[i]=ptrArry[i];*

Eg. Algorithm BioAPI initialize:

*pnParamInit[19]= 0; // Automatic cloud*

*nRet = CgtBioAPI\_Initialize(pDataBuf, nDataSize, pLicConfigPara, pnParamInit, pszMsg);*

Eg. Algorithm Fingerprint API initialize:

*pnParamInit[109]= 0; // Automatic cloud*

*nRet = CgtFinger\_Initialize(pDataBuf, nDataSize, pLicConfigPara, pnParamInit, pszMsg);*

Eg. Algorithm Face API initialize:

*pnParamInit[109]= 1; // Automatic clound*

*nRet = CgtFace\_Initialize\_Ex(pDataBuf, nDataSize, pLicConfigPara, pnParamInit, pszMsg);*