

DISCLAIMER

IDEMIA is warning all the users of this product that the conditions of use of this product are described in the agreement defined between IDEMIA and his customers.

As part of such conditions, it is forbidden to do reverse engineering on the product and / or to upload / copy the product to external entities and by doing so, to confer by agreement such external entities the right to perform inappropriate actions on the product while this right has not been granted by IDEMIA through writing.

This warning applies also to IDEMIA users.

Multiprotect License Protection User's Guide

Version 6.5.0

Reference: 2024_2000078901

INDUSTRIAL PROPERTY RIGHTS

The information contained in this document is the property of IDEMIA. It is confidential and distributed with a specific aim.

The recipient shall ensure the proper safekeeping and monitoring of this document and agrees neither to copy nor reproduce it, in whole or in part, or to reveal its contents to third parties, except in order to further the aim for which the document was provided for them.

This applies to all pages of this document.

Table of contents

1) Release history.....	4
2) Introduction.....	8
2.1) Description.....	8
2.2) Supported protections	8
2.3) Supported platforms.....	9
2.4) Compatibility between different versions of the protection.....	10
2.5) Compatibility between a token server and Multiprotect License Protection	10
3) Installing Multiprotect License Protection application	11
3.1) Drivers installation for Hardware protection type.....	11
3.1.1) SafeNet dongle installation	11
3.1.1.1 SafeNet dongle on Linux	11
3.1.1.2 SafeNet dongle on Windows	11
3.1.2) MorphoDongle installation	14
3.1.2.1 MorphoDongle on Linux Ubuntu	14
3.1.2.2 MorphoDongle on Linux RHEL/CentOS/OL	15
3.1.2.3 MorphoDongle on Windows.....	15
3.2) Multiprotect License Protection installation	16
3.2.1) Installing Multiprotect on Windows	16
3.2.1.1 Silent mode installation.....	18
3.2.1.2 Uninstalling Multiprotect.....	18
3.2.1.3 Downgrading Multiprotect	18
3.2.2) Installing Multiprotect on Linux	18
3.2.2.1 RPM Linux installation procedure	19
3.2.2.2 Debian (Ubuntu) installation procedure	19
3.2.2.3 Installing Multiprotect manually on Linux	20
3.2.2.4 Work directory on Linux	20
3.2.3) Installing Multiprotect on Android	21
4) Installing licenses	21
4.1) Checking licenses availability	21
4.1.1) Licenses availability on Windows	22
4.1.2) Licenses availability on Linux	23
4.1.3) Licenses availability on Android	24
4.2) Adding new license.....	24
4.2.1) Adding new licenses on Windows.....	25
4.2.2) Adding new licenses on Linux.....	27
4.2.3) Adding new licenses on Android	27
4.3) Getting a license	28

4.3.1) Obtaining hostID on Windows	28
4.3.2) Obtaining hostID on Linux	30
4.3.3) Obtaining hostID on Android	30
5) Configuring Multiprotect License Protection application	31
5.1) Configuration principle	31
5.2) Communicating with a remote Token server	31
5.2.1) Communicating with Sentinel® RMS token server	31
5.2.2) Communicating with IDEMIA Multiprotect Token Server/MPaaS	32
5.3) List of configuration parameters.....	34
5.4) List of environment variables.....	39
6) How-To	40
6.1) How to Start/Stop/check Multiprotect License Protection service	40
6.1.1) Start/Stop/check Multiprotect License Protection service on Windows	40
6.1.2) Start/Stop/check Multiprotect License Protection service on Linux	40
6.2) How to know which Multiprotect version is installed?	40
6.2.1) Which Multiprotect version is installed on Windows?	40
6.2.2) Which Multiprotect version is installed on Linux?	40
6.2.3) Which Multiprotect version is installed on Android?	41
6.3) How to reduce memory footprint?	41
6.4) How to enable logs?	41
6.5) How to manually register Multiprotect as a Windows service?	41
7) Troubleshooting	43
7.1) Standalone software license and firewire IEEE 1394 on Windows	43
7.2) Standalone software license and bonding Ethernet interface	43
7.3) Standalone software license with laptop computer	43
7.4) Standalone software license on Linux and usb0 management console	43
7.5) Standalone software license and Virtual Machine.....	44
7.6) Software license with more than one Ethernet Card.....	44
7.7) Software license have been installed successfully but is no longer valid	44
7.8) Best practice for standalone license installation.....	44
7.9) hostID of software license has following format : 2004-*xxxxxxxxxxxxxxxx	44
7.10) Add software license success but did not see any license.....	45
7.11) A software license which has been installed is not valid after a reboot.....	45
7.12) Cannot retrieve a network license from remote license server	45
7.13) Dongle protection is not working	45
7.14) Multiprotect service is consuming 100% of the CPU (rare case on Linux).....	45
7.15) License is no more present on my Android phone	46

1) Release history

6.5.0 (05/2024)

- New features
 - Linux: MorphoDongle is enabled by default
 - Linux: RPM installer upgrade for OS with fips enabled
 - Linux: `-all` option is available for Multiprotect_Manager tool
 - Public COTS upgrade
- Bug fix
 - Windows: small memory leak if MTop 100 is kept plugged
 - Linux tx2: incorrect hostID retrieval when dummy card is listed
- Removed
 - Android: remove thrift support thus support of Android 4.x to 7.x and armv7 devices
 - Windows: remove support of Windows 7 and Windows Server 2012
 - Linux: remove support of Ubuntu 16.04
- Known limitations
 - Windows: license updated/added not seen until device is unplugged/plugged (TOP Slim V3, TOP Slim V2)

6.4.1 (12/2023)

- Bug fix
 - Reading/writing error with some MorphoDongle

6.4.0 (10/2023)

- New features
 - Support new MorphoDongle
 - Public COTS upgrade (openssl, ACS driver for windows)
 - Support Android 14
- Bug fix
 - none
- Removed
 - none
- Known limitations
 - Windows: license updated/added not seen until device is unplugged/plugged (TOP Slim V3, TOP Slim V2)
 - Windows: MSO device not detected after resuming from sleep mode

6.3.0 (08/2023)

- New features
 - Support Windows 11
 - Support Linux 9 (Oracle Linux & RedHat)
 - Public COTS upgrades
 - Support MTOP SlimV3 for Android / Idscreen60
- Bug fix
 - Windows: USB dongle detection plug&play
 - Linux: Start error on Ubuntu 20.04
- Removed
 - View/add license in MorphoAccess devices. Please use MBTB instead
- Known limitations
 - Windows: license updated/added not seen until device is unplugged/plugged (TOP Slim V3, TOP Slim V2)
 - Windows: MSO device not detected after resuming from sleep mode

6.2.0 (03/2023)

- New features:
 - Support Ubuntu 22.04 LTS

- Public COTS upgrades
 - Bug fixes on expiration date management (standalone, IMTS, MPaaS)
 - Improve documentation for docker/container installation
- Known limitations
 - Windows: license updates/added not seen until device is unplugged/plugged (TOP Slim V3, TOP Slim V2)
 - Windows: MSO device not detected after resuming from sleep mode
- 6.1.1 (02/2023)
 - Bug fix:
 - Better management of expiration date from license server
- 6.1.0 (01/2023)
 - New features:
 - Windows: Support of MSO 33x
 - Windows: Support of Sentinel® HL dongles
 - Public COTS upgrades
 - Bug fix: date format of expiration date was not homogeneous
 - Removed:
 - Windows: remove support of vc10
- 6.0.0 (12/2022)
 - New features:
 - Android: Support of Android 13
 - Public COTS upgrades
 - Removed:
 - Android: remove support ndkr10e
 - Android: remove support of Android 4.x, 5.x, 6.x & 7.x
- 5.7.1 (08/2022)
 - New features:
 - Safenet dongle driver upgrade for Windows
 - Windows: Support of MTop 2020
 - Windows: Support of MTop Slim V3
 - Known limitations
 - Android API level>30 not supported on armv7 platforms
- 5.7.0 (07/2022)
 - New features:
 - Public COTS upgrade
 - Support Windows server 2022
 - IDEMIA Multiprotect Token Server/MPaaS token information is now displayed in License Manager
 - Bugs fixes:
 - Multiprotect loses the licenses if network card is lost and then recovered
 - Removed:
 - (Linux) *Multiprotect_Admin*, *Multiprotect_Install_Test* & *Install_Multiprotect.sh* are removed
 - Known limitations
 - Android API level>30 not supported on armv7 platforms
 - (Windows) license updates/added not seen until device is unplugged/plugged (MTop 2020, MTop Slim V3, MTop Slim V2, MTop 100)
 - Starting Multiprotect v6.0.0, android ndkr10e will be replaced by ndkr19c
- 5.6.0 (03/2022)
 - New features:
 - Windows: Support of MTop 2020
 - Windows: Support of MTop Slim V3
 - Windows: IDEMIA COTS upgrade (MLS SDK 4.1.1.0)
 - Bugs fixes:
 - Improve overall stability
 - Known limitations

- Android API level>30 not supported on armv7 platforms
- 5.5.0 (12/2021)
 - New features:
 - Android: Support of Android 11 & 12
 - Removed:
 - Android: License_Admin apk not delivered anymore
 - Known limitations
 - Android API level>30 not supported on armv7 platforms
- 5.4.0 (08/2021)
 - New features:
 - Support of communication with pool of IDEMIA Multiprotect Token Servers (IMTS)
- 5.3.0 (07/2021)
 - New features:
 - Support of Ubuntu 20.04 LTS
 - Linux: default work directory (used for lock file and log files) is changed from `/usr/sbin/Multiprotect` to `/var`
 - New parameter keys available: `<mepLicensesPath>`, `<tx2LicensesPath>`, `<useTx2Protection>`, `<multiprotectLockPath>`
 - New environment variable available: `<MP_CONF_DIR>`
 - Updated:
 - Tool to retrieve hostID is renamed (from `GetSoftStandaloneLockCode` into `GetSoftLockCode`)
 - Linux: parameter key updated `<logDirectory>`
 - Bugs fixes:
 - Incorrect management of license expiration
 - Incorrect management of scan counter
 - Grace period persistence file does not retain license parameters
- 5.2.1 (01/2021)
 - New features:
 - Added support of Windows Server 2019
 - Added support of Red Hat Linux 8.x
 - Add `json_headerHost` parameter (remote webserver communication)
 - Updated:
 - update §Compatibility between client and server
 - Windows: MSO SDK updated (6.33.0 to 6.36.1)
 - Android: merge of ndkr19c APKs into a single APK for easier deployment
 - Bugs fixes:
 - Windows: MSO detection is improved
 - Linux: avoid having `mpld` & `Multiprotect.service` running at the same time
- 5.2.0 (11/2020)
 - New features for remote webserver communication (MPaaS):
 - Linux client info sent to webserver in GPB format
 - improve license error management in case of configuration mistakes
 - separate token's life duration and client info frequency
 - decrease retry counter to reduce network footprint
 - Multiprotect client behind a secured proxy: add proxy parameters
 - Bugs fixes:
 - string format of installed licenses was changed
- 5.1.4 (10/2020)
 - New features:
 - Windows: multiprotect setup includes `vcaredist14` for automatic installation
 - Linux: support of SafeNet dongle on Ubuntu 18.04
 - Linux & Windows: multiprotect upgrade is now available
 - Android: Multiprotect client build info are now available in apk
 - Android: GUI enhancements of License_Admin apk

- Android: Capability to identify OS version at apk launch to prevent compatibilities problems
- Updated:
 - update installation procedure of MorphoDongle on linux
 - set enable_22x_compatibility and enable_3x_compatibility to false by default
- Bugs fixes:
 - Linux: if pipe is broken, service could consume 100% of CPU (rare case)
 - Linux: MorphoDongle ACR3xT was not detected in Linux
 - Android: improve overall stability
 - Windows: "Add license" feature was not working properly
 - Windows: if no internet access, Multiprotect service was not starting in smooth manner

5.1.2 (08/2020)

- Android (from 5 to 10):
 - Support of Android 10 added (armv7, armv8, arm64-v8a)
 - New ndk19c delivery is using Android API level 27 with following features:
 - Add QR code generation for hostID
 - Improve GUI of android applications
 - MSO SDK updated (6.26.0 to 6.33.0)
- Windows:
 - vcredist14 is required
 - MSO SDK updated (6.26.0 to 6.33.0)
- Dongles:
 - From now on, SafeNet dongle or MorphoDongle must be plugged in before Multiprotect starts
 - Only MorphoDongle ACS is supported (HID no longer supported)
- Added a disclaimer regarding Multiprotect License Protection usage
- Drivers for MSO, MTop & MorphoDongle are not delivered in Multiprotect package anymore
- User Guide updated (supported OS, troubleshooting§, etc.)

5.0.2 (06/2019) on Windows / Linux

- Android support with access to remote webserver (MPaaS)

5.0.0 (04/2019) on Windows / Linux

- Add protocol Multiprotect as a Service protection
- NOTE: AIX / Android / iOS / Windows Phone not supported

2) Introduction

Multiprotect License Protection is a component which manages different protection types (with external hardware protection device or machine-lock protection). It stores licenses and made them available to other IDEMIA components to allow/deny access to specific functions.

If an IDEMIA component, which uses Multiprotect License Protection, does not work, you have to:

1. Install Multiprotect License Protection
2. Ask for licenses to IDEMIA (or use a preloaded hardware such as a dongle or MSO) (licenses definition and licenses use are defined by each component).
3. Install licenses provided by IDEMIA

Multiprotect License Protection is available on Windows, Linux and Android platforms.

2.1) Description

Multiprotect License Protection is composed essentially of 3 elements:

- A **service/daemon** which collects licenses available and allows others components to ask for specific licenses
- A **Manager** (Graphic UI or console) which shows the installed licenses and stores new licenses in the protection's hardware
- A **tool** to install licenses concatenated in a file (useful for deployment on a large set of computers)

Tool	Windows	Linux	Android
Service	X	X	X
Manager (GUI)	X		X
Manager (Console)	X	X	

fig1. Multiprotect License Protection components availability by platform

2.2) Supported protections

Multiprotect License Protection supports the following protections (fig2):

- MorphoDongle (hardware)
- MSO (IDEMIA single fingerprint sensor - hardware)
- SafeNet Dongle (hardware)
- MTop 100, MTop 2020, MTop Slim V2, MTop Slim V3 (IDEMIA multiple fingerprint sensor - hardware)
- Software/standalone (Machine-locked) protection (associated with computer or terminal) – **not compatible with Virtual Machine**
- Network licenses:

- RMS token server (to be deployed on premises)
- IDEMIA Multiprotect Token Server (MPaaS to be accessed over internet or to be deployed on premises)

Protection	Type
MorphoDongle	Hardware
MSO	Hardware
SafeNet Dongle	Hardware
MTop 100, MTop 2020	Hardware
MTop Slim V2, MTop Slim V3	Hardware
Machine locked (Software/Standalone)	Software
Network	Software

fig2. Types of the protections

2.3) Supported platforms

Multiprotect License Protection is available for the following platforms (fig3):

- Microsoft Windows Server 2022, 2019 and 2016 (x64),
- Microsoft Windows 11 (x64) and 10 (x64),
- Red Hat, Oracle Linux 9.X (x64), 8.X (x64) and 7.X (x64),
- Ubuntu 22.04 LTS, 20.04 LTS and 18.04 LTS (x64),
- Android from 14 to 8 (ndk19 intent delivery)

Protection	Windows	Linux	Android
MorphoDongle	X	X	
MSO/CBM	X		X
SafeNet Dongle	X	X	
MTop 100, MTop 100 R, MTop 2020, MTop Slim V2	X		
MTop Slim V3	X		X (a)
Machine locked (Software/Standalone)	X	X	X
Network - RMS token server	X	X	
Network – IDEMIA Multiprotect Token License server/MPaaS	X	X	X

fig3. Protection availability by platform

(a): only read license in the device scenario

2.4) Compatibility between different versions of the protection

An old client can always talk to latest version of the protection but a new client might not communicate with an old version of the protection.

Current version is compatible with all client versions from v3.3 onwards.

2.5) Compatibility between a token server and Multiprotect License Protection

As described in chapter §2.2), 2 network modes are supported by Multiprotect License Protection:

- Sentinel® RMS token server
- IDEMIA Multiprotect Token Server/MPaaS

Since Multiprotect License Protection v5.0.0, both network modes are supported (for configuration, see chapter §5.2) however, Multiprotect License Protection v4.x supports only RMS token server.

An old daemon can always use a new token server, but a new daemon may have compatibility issues with an old token server.

3) Installing Multiprotect License Protection application

3.1) Drivers installation for Hardware protection type

This section applies to Hardware Protections (see list of support Hardware Protections in chapter §2.2). If you need Hardware Protections, please install the associated driver on your system before deploying the Multiprotect License Protection software.

3.1.1) SafeNet dongle installation

3.1.1.1 SafeNet dongle on Linux

To install SafeNet dongle driver, launch `.sh` script provided with Safenet Dongle driver.



Since Multiprotect License Protection v5.1.x, dongle must be plugged before Multiprotect application starts.

3.1.1.2 SafeNet dongle on Windows



Do not plug your dongle before installing driver otherwise dongle might not be detected.



You should be logged as an administrator to install drivers or run setup as an administrator.

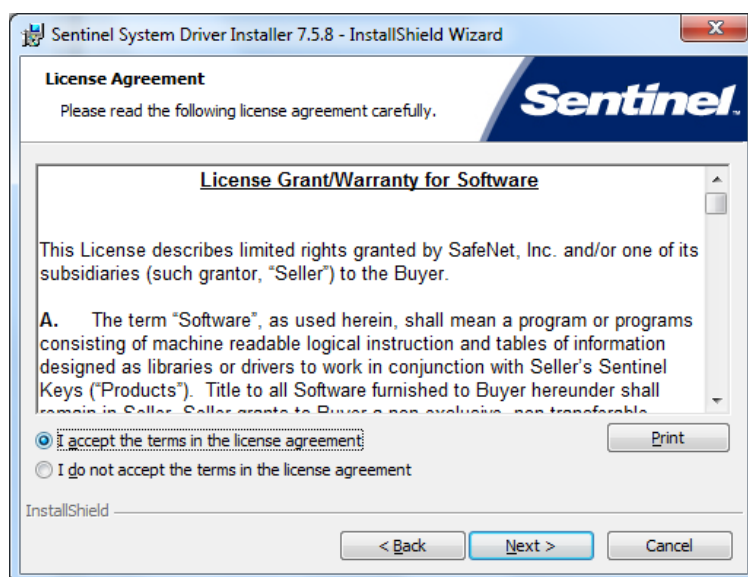


Please use latest version of driver provided with the SafeNet dongle.

Launch *Sentinel® System Driver Installer x.y.z.exe* and follow InstallShield Wizard steps described below:

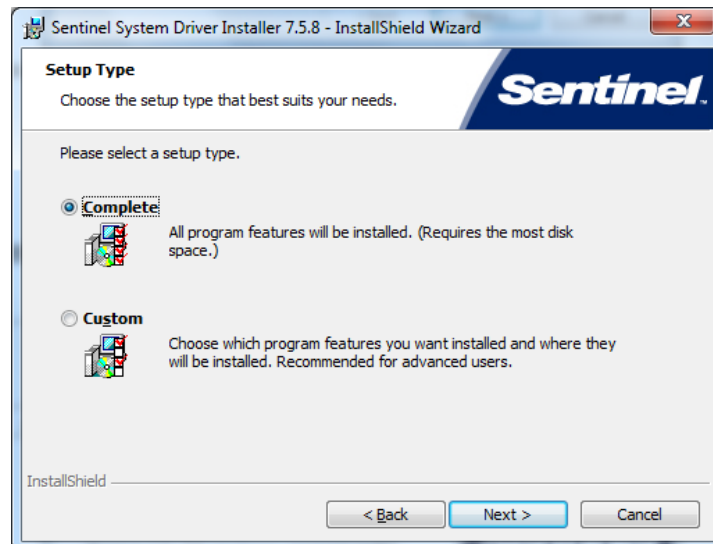


Click on **Next** button.

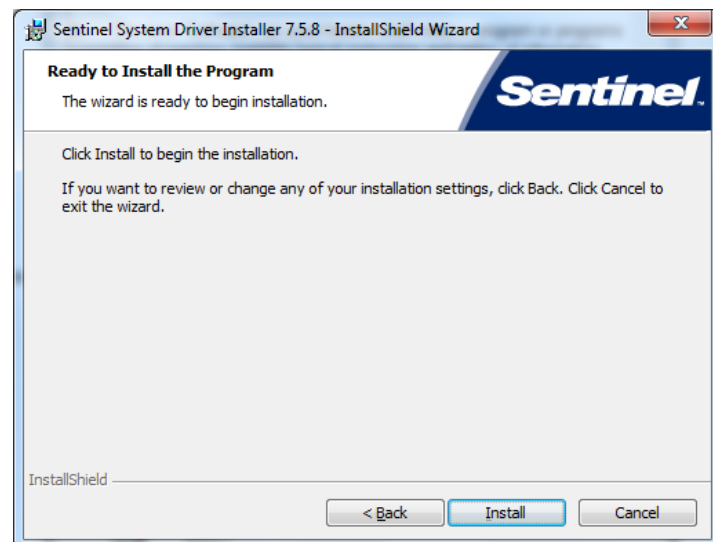


Select "I accept the terms in the license agreement" and click on **Next** button.

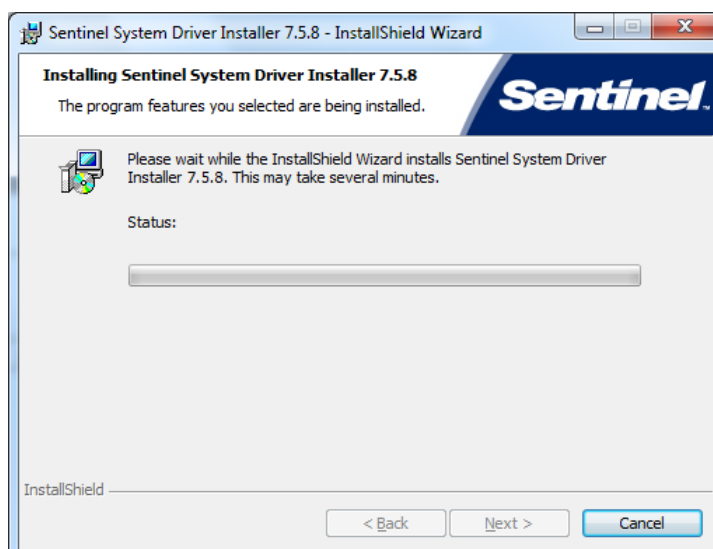
Sentinel® is a registered trademark of Thales, Inc.

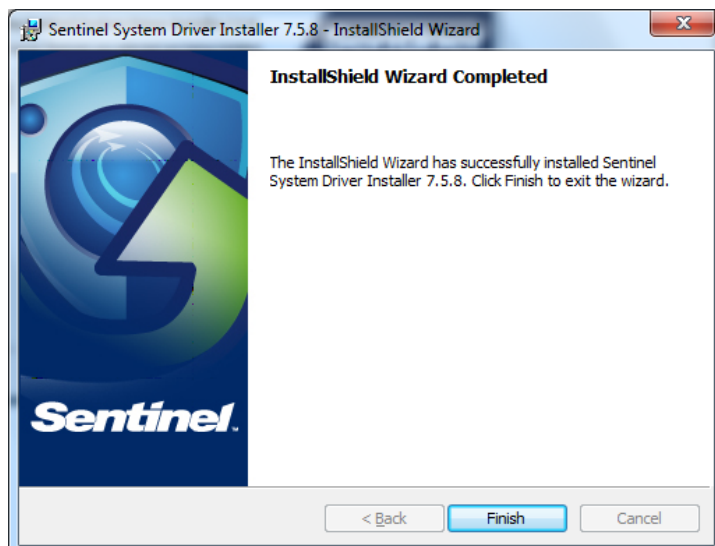


Select **Complete** choice and click on **Next** button.



Click on **Install** button.





When installation has been successfully performed, click on **Finish** button.

NOTE

Since Multiprotect License Protection v5.1.x, dongle must be plugged before Multiprotect application starts.

3.1.2) MorphoDongle installation

Multiprotect supports MorphoDongle with ACS ACR38T and ACR39T readers.

3.1.2.1 MorphoDongle on Linux Ubuntu

Required packages:

- PCSC daemon (**pcscd**) and libraries (**libpcsc-lite**): Middleware to access a smart card using PC/SC.
- CCID driver (**libccid**): Generic USB CCID (Chip/Smart Card Interface Devices) driver

Package installation on Ubuntu:

```
apt-get install pcscd
```

(the required libraries are added as dependencies of the daemon)

To use MorphoDongle protection, it is **NECESSARY** that:

- pcsc daemon (**pcscd**) is started
- *app_conf* file is added in the directory which contains Multiprotect binary. Add in it: **useMorphoDongle=1** and restart the service.

NOTE

Since Multiprotect License Protection v5.1.x, dongle must be plugged before Multiprotect application starts.

3.1.2.2 MorphoDongle on Linux RHEL/CentOS/OL



MorphoDongle does not work on RHEL 5.X

Required packages:

- PCSC daemon (**pcscd**) and libraries (**libpcsc-lite**): Middleware to access a smart card using PC/SC.
- CCID driver (**libccid**): Generic USB CCID (Chip/Smart Card Interface Devices) driver

Package installation on RHEL/CentOS/OL:

```
yum install pcsc-lite
```

(the required libraries are added as dependencies of the daemon)

To use MorphoDongle protection, it is **NECESSARY** that:

- pcsc daemon (**pcscd**) is started
- *app_conf* file is added in the directory which contains Multiprotect binary. Add in it: **useMorphoDongle=1** and restart the service.
- For RHEL 6.x, the package **opent** must be uninstalled using the command

```
rpm -e -nodeps
```

 otherwise MorphoDongle is not recognized (there is an incompatibility issue between opent and ACR38 driver)



Since Multiprotect License Protection v5.1.x, dongle must be plugged before Multiprotect application starts.

3.1.2.3 MorphoDongle on Windows



Since Multiprotect License Protection v5.1.x, dongle must be plugged before Multiprotect application starts.

On Windows 10 and upper versions, there is no need to install a driver to use ACS SIM card reader. You can skip this step.

For others Windows OS versions, please launch *Setup.exe* located in **drivers\MorphoDongle** directory.



Do not plug your dongle before installing driver otherwise dongle might not be detected.



You should be logged as an administrator to install drivers or run setup as an administrator.

3.2) Multiprotect License Protection installation

3.2.1) Installing Multiprotect on Windows

This paragraph describes the installation steps of Multiprotect License Protection on Windows.

Multiprotect License Protection runs as a Windows service and is by default automatically registered in Windows and launched.

Procedure:



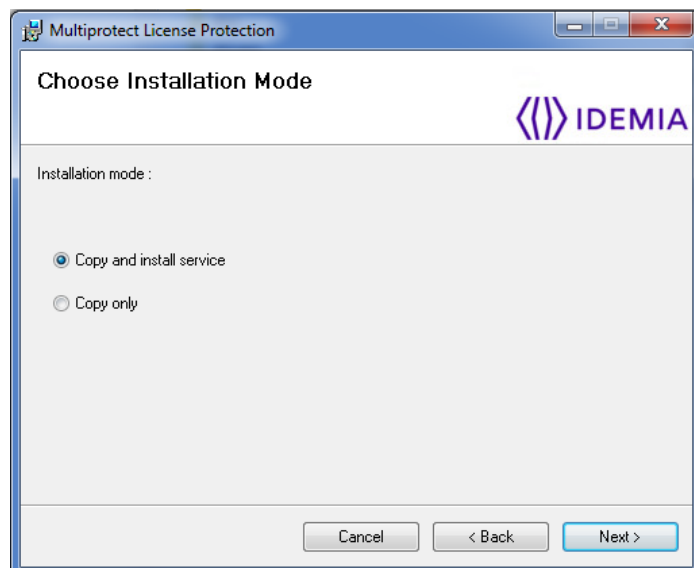
VERY IMPORTANT: You must install Multiprotect License Protection software with Administrator rights.

Launch *Multiprotect_License_Protection_Installer.msi* with administrator rights (right click on mouse button and click on "**Install**").

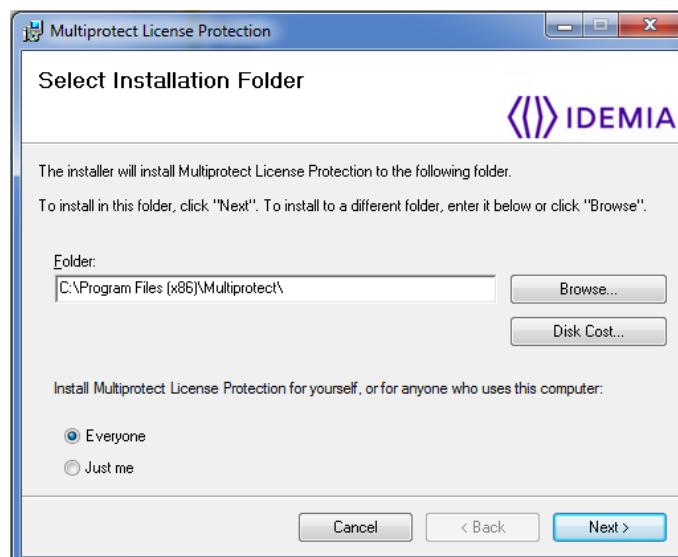


Choose installation mode. Unless there is an error during installation, choose "**copy and install service**".

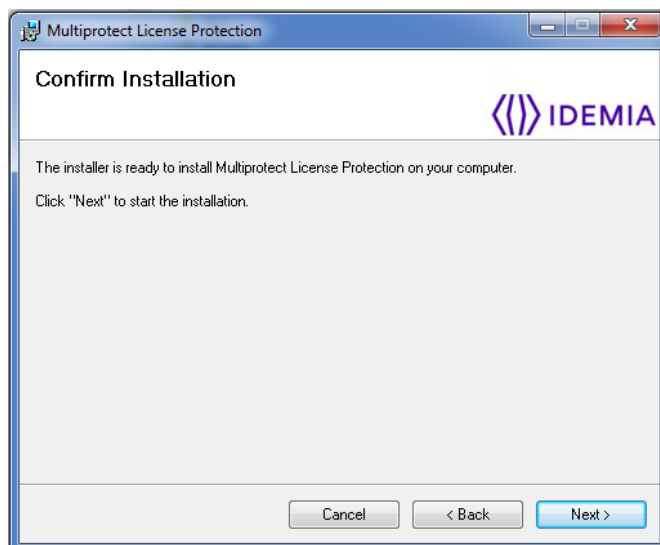
NOTE: If you choose "copy only" option, then license service **will not be registered in Windows**.



Select Installation folder:



Confirm installation:



3.2.1.1 Silent mode installation

Please execute following commands as an administrator:

```
msiexec /i Multiprotect License Protection Installer.msi /quiet
```

3.2.1.2 Uninstalling Multiprotect

There are three possibilities to uninstall Multiprotect:

- 1) Go to add/remove programs in windows configuration panel and uninstall "*Multiprotect License Protection*".
- 2) Run the shortcut in "Start / All Programs / Multiprotect / Uninstall Multiprotect License Protection".
- 3) Run the *uninstall.bat* in the installation directory (by default in **C:\Program Files\Multiprotect**)

3.2.1.3 Downgrading Multiprotect

Downgrade of Multiprotect License Protection is not supported.

If you want to install an old version, please uninstall the application manually.

3.2.2) Installing Multiprotect on Linux



We strongly recommend using RPM installation on the system where RPM is the default package format. For Ubuntu, we recommend to use .deb package.

3.2.2.1 RPM Linux installation procedure

A full RPM is delivered (*multiprotect-x.x.x-1.abc.rpm* where x.x.x is version and abc is the platform).

Prerequisites:



- **VERY IMPORTANT:** You must be logged as root to install the application.
- On OL or RHEL, please verify that these packages are installed:
libgudev1.x86_64, libgudev1-devel.x86_64

Procedure:

Please install Multiprotect License Protection with following yum command so libraries **glibc.i686, compat-libstdc++-33.i686** and **libstdc++-i686** would be installed automatically:

```
yum install -y multiprotect-x.x.x-1.abc.rpm
```



In container/docker, please ensure `LD_LIBRARY_PATH` is defined and is the running directory of Multiprotect.

Protection's daemon is created and respawned automatically.

3.2.2.1.1 Uninstalling Multiprotect

To uninstall Multiprotect License Protection, execute the following command in the terminal console:

```
yum erase -y multiprotect
```

3.2.2.1.2 Downgrading Multiprotect

Downgrade of Multiprotect License Protection is not supported. If you want to install an old version, please uninstall the application manually.

3.2.2.2 Debian (Ubuntu) installation procedure

A DEB is delivered (*multiprotect_x.x.x_abc.deb* where x.x.x is version and abc is the platform).

Prerequisites:



- **VERY IMPORTANT:** You must be logged as root to install the application
- please verify that this package is installed: **libudev1**

Procedure:

1/ Install dependencies. You can launch these two commands:

```
apt-get install -y libc6-i386 lib32stdc++6 lib32gcc1 lib32ncurses5 lib32z1
dpkg --add-architecture i386
```

2/ Follow standard dpkg installation: `dpkg -i multiprotect_x.x.x_abc.deb`

NOTE In container/docker, please insure `LD_LIBRARY_PATH` is defined and is the running directory of Multiprotect.

Protection's daemon is created and respawned automatically.

3.2.2.2.1 Uninstalling Multiprotect

To remove protection from dpkg, launch following command in terminal console:

```
dpkg -P multiprotect
```

3.2.2.2.2 Downgrading Multiprotect

Downgrade of Multiprotect License Protection is not supported.

If you want to install an old version, please uninstall the application manually.

3.2.2.3 Installing Multiprotect manually on Linux

If you want to do a manual installation (like an RPM, or for a container deployment):

- 1/ You have to include every binary available in `bin` folder
- 2/ Then `Multiprotect_License_daemon` must be started as root during boot. Other users could also be used but root user is our recommended option (validation of component is made with root user only).
- 3/ Please insure `LD_LIBRARY_PATH` is defined and is the running directory of Multiprotect.
- 4/ (optional) please add some directories creation as mentioned in §3.2.2.4

3.2.2.4 Work directory on Linux

Work directory (for lock file and log files) is `/var` as follow:

- `/var/log/mp` for Multiprotect trace/log files (created by Multiprotect License Protection installer)
- `/var/run` for lock file `multiprotect.lock`

If you want to change work directory, please use `<multiprotectLockPath>` & `<logDirectory>` parameters defined in chapter §5.3).



NOTE Prior to Multiprotect License Protection v5.3.0, work directory was `/usr/sbin/Multiprotect`

3.2.3) Installing Multiprotect on Android



If smartphone is rooted, no license will be available

To use Multiprotect application on Android, 2 APKs are delivered:

APK filename		Description
<i>Multiprotect_License_Protection.apk</i> (mandatory)		Main application to manage licenses. Called 'daemon'
<i>Multiprotect_License_Manager.apk</i> (optional)		This application has graphical user interface to install licenses, read hostID & available licenses

Procedure:

Once "**License Service**" is installed, please click on License Service icon to launch it or you can also restart your device.



Installation of these APKs may require that you enable installation of apk from unknown source. You can temporarily enable this feature and disable it when installation is over. These APKs do not contain any unsafe element.

4) Installing licenses

This section describes the licenses generation procedure and the licenses used by Multiprotect License Protection.

4.1) Checking licenses availability

To check the availability of the licenses, open Multiprotect Console License Manager. It will automatically detect all available licenses and a detailed description of licenses.

4.1.1) Licenses availability on Windows

In Windows, there are 2 ways: **Multiprotect License** GUI or **Windows console**.

Multiprotect License GUI

From Windows *Start Menu* Button, select *Multiprotect License Manager (GUI)* application



Multiprotect License Manager (GUI) application will list the Installed License as follow:

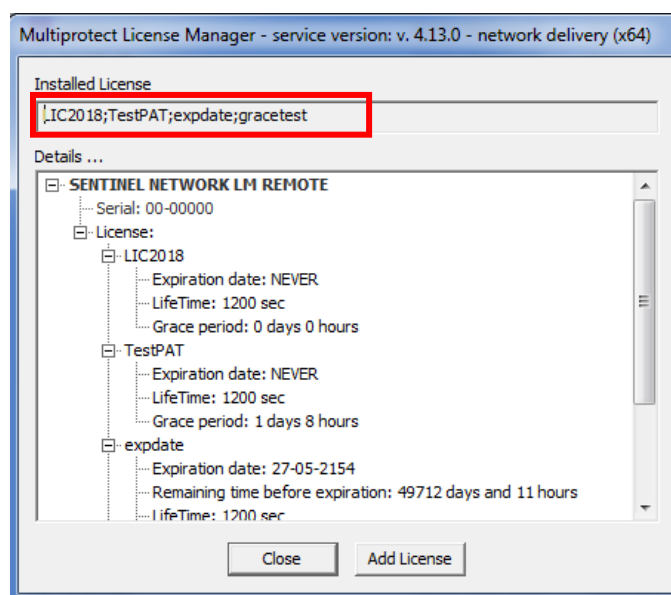


fig4. Multiprotect License Manager (Windows GUI version)

Windows console

In a Windows DOS console, type the following commands:

```
cd C:\Program Files\Multiprotect
Multiprotect Console License Manager.exe
```

`-all` option can provide detailed information for each license.

Multiprotect Console License Manager will list the Installed License as follow:

```
C:\Windows\System32\cmd.exe - Multiprotect_Console_License_Manager.exe -all
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Program Files\Multiprotect>Multiprotect_Console_License_Manager.exe -all

Multiprotect Console License Manager

Service version: v. 4.13.0 - network delivery <x64>
Installed: LIC2018;TestPAI;expdate;gracetest

Details :
+ SENTINEL NETWORK LM REMOTE
|- Serial: 00-00000 (Server mode)
|- Licenses:
|-|- LIC2018
|-|-|- Expiration date: NEVER
|-|-|- LifeTime: 1200 sec
|-|-|- Grace period: 0 days 0 hours
|-|-|- TestPAI
|-|-|- Expiration date: NEVER
|-|-|- LifeTime: 1200 sec
|-|-|- Grace period: 1 days 8 hours
|-|- expdate
|-|-|- Expiration date: 27-05-2154
|-|-|- Remaining time before expiration: 49712 days and 11 hours
|-|-|- LifeTime: 1200 sec
|-|-|- Grace period: 1 days 20 hours
|-|- gracetest
|-|-|- Expiration date: NEVER
|-|-|- LifeTime: 1200 sec
|-|-|- Grace period: 1 days 1 hours
```

fig5. Multiprotect License Manager (Windows Console version)

4.1.2) Licenses availability on Linux

Execute the following command from a terminal:

`Multiprotect_Manager`

`-all` option can provide detailed information for each license.

Multiprotect Console License Manager will list the Installed License as follow:

```
root@multiprotect-VirtualBox: /usr/sbin/Multiprotect

Multiprotect Console License Manager

Service version: v. 4.13.0 - network delivery (x86)
Installed: gracelic

Details :
+ SENTINEL NETWORK LM REMOTE
|- Serial: 00-00000 (Server mode)
|- Licenses:
|-|- gracelic
|-|-|- Expiration date: NEVER
|-|-|- LifeTime: 1200 sec
|-|-|- Grace period: 1 days 1 hours
```

fig6. Multiprotect License Manager (Linux Console version)

4.1.3) Licenses availability on Android



If smartphone is rooted, no license will be available

Launch the Multiprotect License Manager application to display the licenses available:

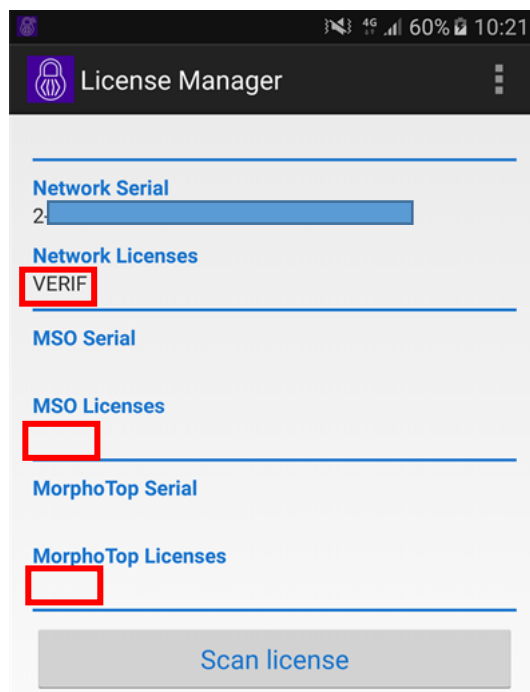


fig7. Multiprotect License Manager (Android GUI version)



4.2) Adding new license

This section **does not apply** to licenses retrieved from remove license server. Please refer to chapter §5.2) for communicating with a remote Token server.

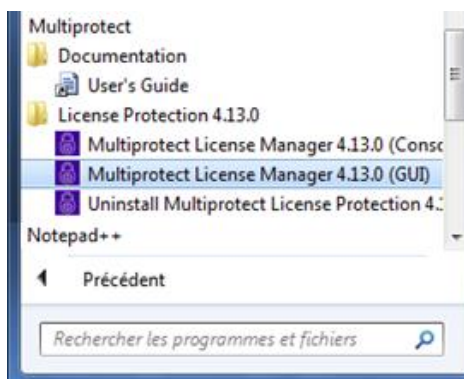
Pre-requisites: IDEMIA had generated a license for your machine (see chapter §4.3).

4.2.1) Adding new licenses on Windows

In Windows, there are 3 ways: **Multiprotect GUI**, **Windows console**, **specific directory**.

Adding new licenses via Multiprotect License GUI

From Windows *Start Menu* Button, select *Multiprotect License Manager (GUI)* application



Click on the "add license" button. A new window appears:

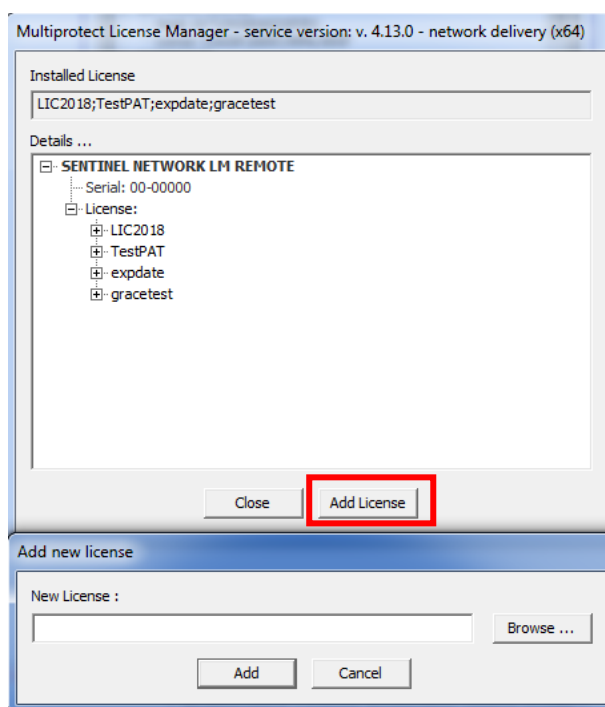


fig8. Add licenses with Windows GUI

Click the "*browse*" button then an open file dialog appears. Choose the license file provided by IDEMIA.

You can control installed license thanks to chapter §4.1).

Adding new licenses via windows console

In a Windows DOS console, type the following commands:

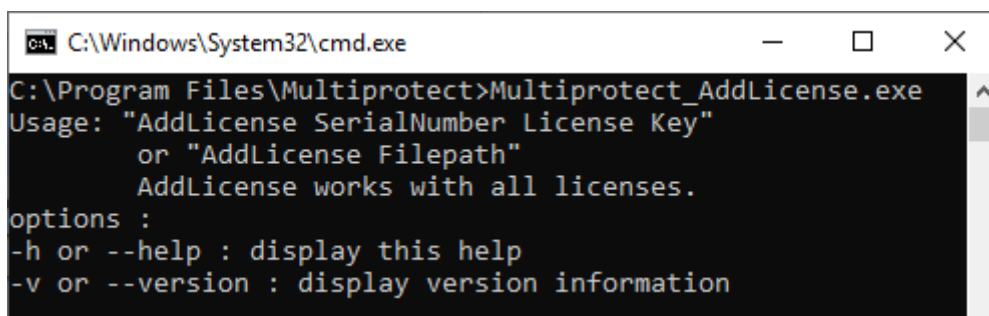
```
cd C:\Program Files\Multiprotect
Multiprotect AddLicense.exe
```

Its usage is:

```
Multiprotect AddLicense SerialNumber License Key
Multiprotect AddLicense LicenseFile
```

LicenseFile is the name of the file containing the license to add.

Multiprotect_AddLicense works with all licenses.



```
C:\Windows\System32\cmd.exe
C:\Program Files\Multiprotect>Multiprotect_AddLicense.exe
Usage: "AddLicense SerialNumber License Key"
      or "AddLicense Filepath"
      AddLicense works with all licenses.
options :
-h or --help : display this help
-v or --version : display version information
```

fig9. Add licenses with Windows console

Examples:

```
Multiprotect AddLicense my_license_file
Multiprotect AddLicense 32327 LIC1;LIC2 A98792371D46A4732A80
```

You can control installed license thanks to chapter §4.1).

Adding new licenses via specific directory

To install a standalone machine-locked (software) license, you can also copy license file called *lservrc* in **c:\licences** folder (This folder is created by this service. You should wait for at least 30 seconds to show licenses).

If you want to change this folder location, please use environment variable **<LSDEFAULTDIR>** as defined in chapter §0.

You can control installed license thanks to chapter §4.1).

4.2.2) Adding new licenses on Linux

On Linux, execute the following command:

```
Multiprotect Add License LicenseFile
```

LicenseFile is the name of the file containing the license to add.

```
root@multiprotect-VirtualBox:/usr/sbin/Multiprotect# ./Multiprotect_Add_Licence
Usage: "AddLicence SerialNumber Licence Key"
       or "AddLicence Filepath"
       AddLicence works with the SafeNet Dongle, Software licences and MorphoTop
       p (on Ubuntu distribution only).
```

fig10. Add licenses with Linux

You can control installed license thanks to chapter §4.1).



To install a machine standalone license file (called *lservrc*), you can also copy *lservrc* file in **Multiprotect_License_Daemon** directory and license will be automatically installed (you should wait for at least 30 seconds to show licenses).



Installing software licenses on linux is not compatible with secure boot.

4.2.3) Adding new licenses on Android

Installing a license can be done in 3 ways:

1. license is a **QR code**: select "scan license" and take a picture of the QR code given by IDEMIA.
2. license is a **file**: copy the license file to the terminal and import in the application (select "add license")
3. license is a **string**: type in the license string and hit "add license"

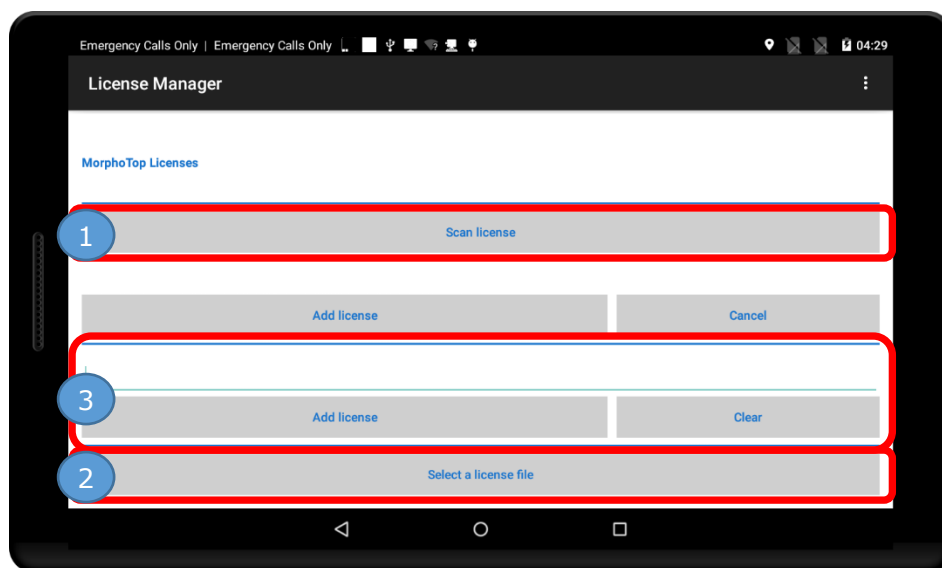


fig11. Add licenses with Android

You can control installed license thanks to chapter §4.1).

On IDEMIA Tablet devices only, CBM (single fingerprint sensor) can be used to store/get licenses.

If you plan to add licenses to CBM sensor, then no fingerprint acquisition should be performed while performing this operation and CBM must be powered on.

4.3) Getting a license

NOTE Reminder: Standalone Software license is **not compatible with Virtual Machine**

IDEMIA needs the **hostID of the machine** in order to generate a license. Please contact IDEMIA representatives by providing hostID of the machine(s).

4.3.1) Obtaining hostID on Windows

In Windows, there are 2 ways: **Multiprotect License** GUI or **Windows console**.

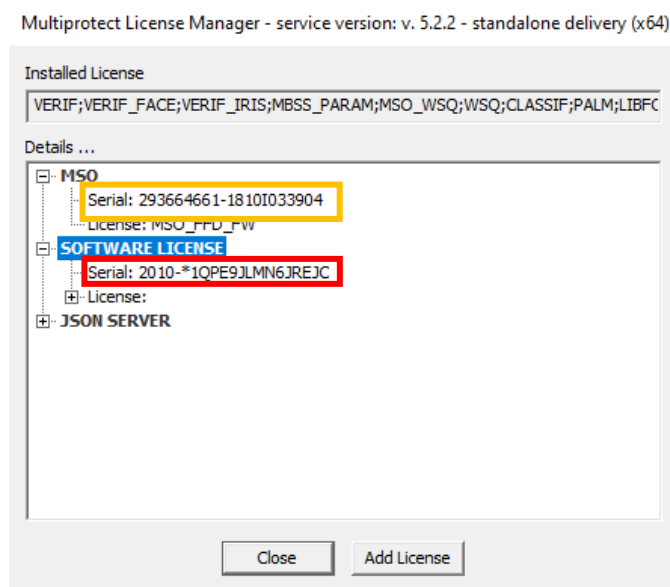
Obtaining hostID via Multiprotect License GUI

From Windows *Start Menu* Button, select *Multiprotect License Manager (GUI)* application:



Several hostIDs (serials) may be available depending on your setup:

- In red: hostID for machine-locked – standalone protection
- In orange: hostID for MSO fingerprint sensor protection



You can copy hostID to clipboard by doing right click on the hostID value.

Obtaining hostID via windows command line



This tool does not need to have Multiprotect License Protection installed.
Recommended for automation of fleet management.

Open the installation package and execute the following commands:

```
GetSoftLockCode.exe
```

It returns the hostID of the machine as follow

```
C:\tools>GetSoftLockCode.exe
Soft Standalone lock code (5.2.2)
code : 2010-*1QPE9JLMN6JREJC
```

fig12. Display hostID via Windows command line

Tool usage is:

```
GetSoftLockCode option
```

```
--help -h           : Display this message
--version -v        : Display protection version used to build tool
-hdd                : Display code linked to hard disk
-allnet             : Display codes for all network cards
-all                : Display all codes
```

4.3.2) Obtaining hostID on Linux

Execute the following command as root:


```
./GetSoftLockCode
```

It returns the hostID of the machine. Otherwise, if `GetSoftLockCode` is executed without root privilege, you will get "Operation not permitted, program needs to be run as root" message.

Tool usage is:

```
GetSoftLockCode option
```

```
--help -h           : Display this message
--version -v        : Display protection version used to build tool
-hdd                : Display code linked to hard disk
-allnet             : Display codes for all network cards
-all                : Display all codes
```

 Installing software licenses on linux is not compatible with secure boot.

4.3.3) Obtaining hostID on Android

Obtaining the hostID on Android can be done in 2 ways:

1. Display a QR code: from the license manager select "Display QR" button,
2. Copy serial to clipboard or file: on the license manager, select settings on the top right corner to have copy options

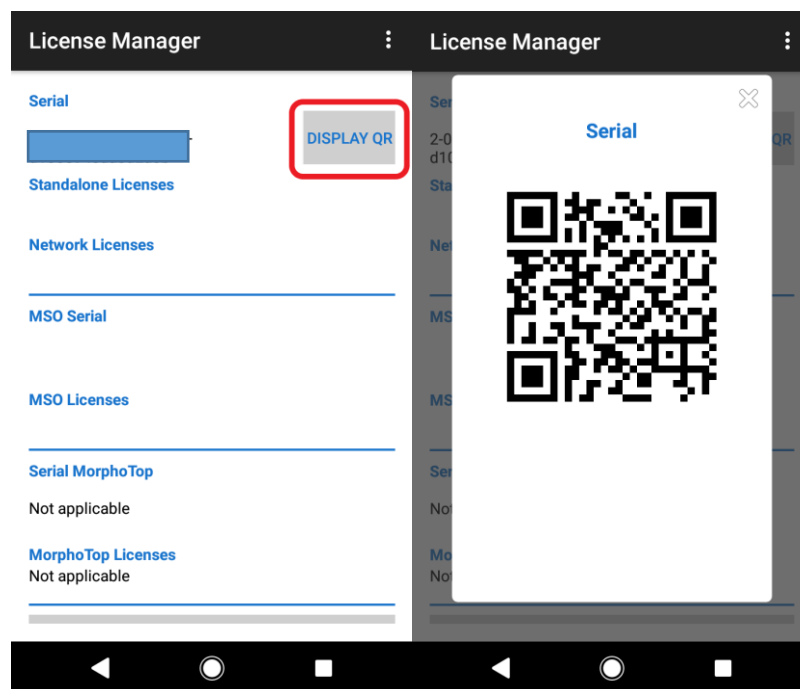


fig13. Display hostID in QR code

5) Configuring Multiprotect License Protection application

5.1) Configuration principle

The configuration of the service is done in *app_conf* file (no extension after this file). By default, configuration file location is:

- for linux environments: */usr/sbin/Multiprotect*
- for windows environments: the execution folder of the service on windows
- for android: *android\data\com.morpho.multiprotectservice\files\MultiprotectConf*

This *app_conf* file may contain network configuration to access token license servers, additional parameters to enable/disable specific protections or to enable logs.



If daemon/service is already launched, please restart the device or daemon/service so that new configuration is used.



For linux environments, if you want the configuration files to be somewhere other than default directory, you can use environment variable **<MP_CONF_DIR>** as follow (see parameter defined in chapter §5.4):

- edit the */etc/systemd/system/Multiprotect.service* file generated after installation
- add following new line

```
Environment=MP_CONF_DIR=<your_configfiles_path>
```

This has the effect to define a new environment variable **<MP_CONF_DIR>** only known inside the service, and not visible outside.

Warning#1: for the service to take into account the modification *Multiprotect.service* file, you must run command: `systemctl daemon-reload`

then `systemctl start Multiprotect`

Warning#2: if Multiprotect is uninstalled, and/or reinstalled, the environment variable is permanently lost. You must enter this variable again in the *Multiprotect.service* file.

5.2) Communicating with a remote Token server

5.2.1) Communicating with Sentinel® RMS token server

As described in 2.3), this mode is not supported for Android environments.

To use following configuration, you have to install on at least one remote machine a token server which can distribute tokens to machines (For Token Server information, please refer to Token Server installation guide).

The configuration must contains at least the following 3 keys:

- **serverSoft:** 0 (disabled, default value) or 1 (enabled)
- **remoteLicence:** list of licenses to ask to remote server. The licenses must be separated by semicolons
- **licenceServer:** the names of the remote servers (2 servers must be set in this field) to interrogate separated by a colon. You can specify the name or the IP address of the servers.



Additional parameters such as communication via a secure web proxy are described in chapter §5.3)



Using Sentinel RMS on linux is not compatible with secure boot.

Example 1:

Here, we will talk to a redundant license server pool (made of 3 servers) and try to get LICENSE1, LICENSE2 and LICENSE3 from this pool of server.

```
# Enable communication with remote server
serverSoft=1
# License list to check on server
remoteLicence=LICENSE1;LICENSE2;LICENSE3
# Servers
licenceServer=<rmsserver1>~<rmsserver2>~<rmsserver3>
```

Example 2:

Here, we will talk to a single token license server pool and try to get LICENSE1, and LICENSE3 from this server.

```
# Enable communication with remote server
serverSoft=1
# License list to check on server
remoteLicence=LICENSE1;LICENSE3
# Servers
licenceServer=<rmsserver1>
```

5.2.2) Communicating with IDEMIA Multiprotect Token Server/MPaaS

To use following configuration, you need access to IDEMIA Multiprotect Token Server/MPaaS (Please contact IDEMIA team to get a project provisioning with the licenses you need).



IDEMIA will provide you a *projectKey*. This project key is sufficient to use your quota of licenses and should be **considered as sensitive**.

Configuration can contain following elements:

- **json_serverSoft:** 0 (disabled, default value) or 1 (connection to IDEMIA Multiprotect Token Server/MPaaS)
- **json_remoteLicence:** the list of licenses to ask to remote server. The licenses must be separated by semicolons
- **json_licenceServer:** the list of IP address or name of the remote servers. Each one is separated by a ~ character
- **json_serverProtocol:** http (default value) or https
- **json_serverPort:** the communication port with remote Server (80, default value)
- **json_projectKey:** the name of the project containing the licenses (given by Multiprotect team during provisioning)
- **json_clearOnExit:** 0 (disabled, persist tokens for reuse, default value on Android) or 1 (enabled, release licenses on exit in MPaaS, default value for other environments – MANDATORY in container mode)

NOTE

Additional parameters such as communication via a secure web proxy are described in §5.3)

Example 1: remote communication to server

Here, we will talk to a Web Server and try to get LICENSE1, LICENSE2 and LICENSE3

```
# Enable communication with remote WebServer
json_serverSoft=1
# License list to check on server
json_remoteLicence=LICENSE1;LICENSE2;LICENSE3
# Web Server
json_licenceServer=<webserver>
# Server Port
json_serverPort=<SERVERPORT>
# Project key
json_projectKey=<PROJECTKEY>
```

Example 2: Hybrid communication

Here, we will talk

- to a Web Server and try to get LICENSE1, LICENSE2
- to a machine-locked RMS Server and try to get LICENSE11, LICENSE12, LICENSE13

```
# 1. Communication with remote WebServer
json_serverSoft=1
json_remoteLicence=LICENSE1;LICENSE2
json_licenceServer=<webserver>
json_serverPort=<SERVERPORT>
json_projectKey=<PROJECTKEY>
# 2. Communication with remote Rms Server
serverSoft=1
remoteLicence=LICENSE11;LICENSE12;LICENSE13
licenceServer=<rmsserver>
```

5.3) List of configuration parameters




Multiprotect relies on a text configuration file to retrieve its run parameters: *app_conf* (no extension, files to be set in the run folder of the Tools)


This page lists and describes the parameters available. All parameters are set in the files on single lines in the form *<parameter>=<value>*



If you add a # character at the beginning of a line, this line is considered as a comment.

Parameter	Values	Default value	Description
runAsService	0 or 1	1	Defines if the binary will launch a forked process in background and exit or run interactive
serverSoft	0 or 1	0	Activates or deactivates (default) the capacity to retrieve license tokens from a Sentinel® RMS server
remoteLicence	list separated by ;		List of licenses to retrieve on the Sentinel® RMS token server
licenceServer	ip or hostnames, separated by ~ or ;		List of servers on which Multiprotect will try to retrieve licenses. In case of Failure, there is a fallback to a broadcast on the local network to discover an available server.
nbMaxTryUpdate	number	4	Maximum number of token update errors before the daemon considers the license lost
nbUpdateOk	number	4	Number of successful updates needed before canceling the error count
serverPort	port number	5093	Port on which the daemon will try to connect
poolSize	number	40 on non arm architectures 1 on arm architectures	number of threads in the pool that the service used to listen to application license requests
thriftPoolSize	number	3	number of threads in the pool that the service used to listen to application license requests (arm architectures only)
poolFrequency	number	10	
max_try	number	10000	maximum number of try in ToolShareServer
request_timeout	number (milliseconds)	60000	timeout value in ToolShareServer

Parameter	Values	Default value	Description
IsDefaultDir	path	C:\\licences (Windows) /usr/sbin/Multi protect (Linux)	Sentinel® LM LSDEFAULTDIR value where the software license file will be looked for
captor_scan_delay	number	10	Limits the scan frequency on MSO/MTop/MTop Slim (default 5min instead of 30s for other protections) -  Added in v4.16.1
global_timeout_read	number (milliseconds)	1000	Timeout on client/server configurations
global_timeout_write	number (milliseconds)	1000	Timeout on client/server configurations
client_timeout_read	number (milliseconds)	1000	Timeout on client/server configurations
client_timeout_write	number (milliseconds)	1000	Timeout on client/server configurations
useMTop	0 or 1	1 if windows 0 on other environments	Do we take into account the licenses available in a connected MTop
useTOPS	0 or 1	1 on Windows 0 on other environments	Do we take into account the licenses available in a connected MTop Slim
lockMultipleCards	0 or 1	0	Do we lock license on all available network cards or only the first one
useSafenetDongle	0 or 1	1 on windows 0 on other environments	Do we allow licenses locked to a Safenet dongle
enable_22x_compatibility	0 or 1	0	Does the daemon accept requests from clients linked to Multiprotect 2.x versions.  Disabled by default from version 5.1.4
enable_3x_compatibility	0 or 1	0	Does the daemon accept requests from clients linked to Multiprotect 3.x versions  Disabled by default from version 5.1.4
enable_4x_compatibility	0 or 1	1	Does the daemon accept requests from clients linked to Multiprotect 4.x versions

Parameter	Values	Default value	Description
useMSO	0 or 1	1	Do we take into account the licenses available in a connected MSO
useMorphoDongle	0 or 1	1 on windows 0 on other environments	Do we take into account the licenses available in a connected MorphoDongle
useSoftLicense	0 or 1	1	Do we take into account the software licenses available
useMepProtection	0 or 1	1 on linux/arm architectures 0 on other environments	Do we take into account the MEP licenses
mepLicensesPath	string	/usr/sbin/Multi protect	Path of MEP standalone license file  Available for Arm64 only, from v5.3.0
changeDirectory	0 or 1	1	
ACR38T_D1	string	"ACS CCID USB Reader 0" on windows "ACS ACR38U-CCID 00 00" on linux "ACS ACR 38U-CCID 00 00" (debian only)	Name of the ACR38 reader accepted for morphodongle access
HID_OMNIKEY	string	"OMNIKEY CardMan 3x21 0" on windows "HID_OMNIKEY", "OMNIKEY CardMan (076B:3021) 3x21 00 00" on linux	Name of the omnikey reader accepted for morphodongle access.
consoleLog	0 or 1	0	set to 1 to have Multiprotect output its log to stdout
enableLog	0 or 1	0	activate or deactivate Multiprotect logs
logLevel	number	0	log level (from 0 to 4, error only to trace level)
logDirectory	path	Linux: /var/log/mp	folder where the log files will be created (defaults to binary folder)

Parameter	Values	Default value	Description
		Other environments: binary folder	<div>NOTE</div> For Linux, default is changed from v5.3.0
enableFiltering	0 or 1	0	allows the definition of filters on which source files will be allowed to output logs
filters	string		list of source files (separator ;) from which logs will be accepted
max_lines	number	50000	maximum number of lines written in a log file before changing file (srv_trace_0.log, then srv_trace_1.log, ...)
json_serverSoft	0 or 1	0	activates or deactivates (default) the capacity to retrieve license tokens from IDEMIA Multiprotect Token Server solution
json_remoteLicence	string		list of licenses to ask to remote server. The licenses must be separated by semicolons
json_licenceServer	ip or hostnames, separated by ~ or ;		IDEMIA Multiprotect Token server(s) on which Multiprotect will try to retrieve licenses (IP address or name of the server). Can be a list of servers if each server is separated by a ~character. In case of Failure, there is a fallback to discover an available server.
json_serverProtocol	string	http	Protocol (http or https)
json_serverPort	number	80	the communication port with Web Server
json_projectKey	string		the name of the project containing the licenses
json_renewThreshold	number	90	the threshold (percentage) at which the tokens are renewed
json_clearOnExit	0 or 1	0 on Android 1 on other environments	<div>NOTE</div> persist tokens on file for reuse (0) or release licenses on exit (1). In container mode, keep default value (1)
json_clientInfo	0 or 1	1	activate or deactivate retrieving license manager information
json_proxy	string		proxy to use to access IDEMIA Multiprotect Token server
json_proxyuser	string		username to authenticate to proxy

Parameter	Values	Default value	Description
json_proxypassword	string		password to authenticate to proxy
json_headerHost	string		DNS name of the "on premises" frontal server (ingress). For example: "licensing.idemia.com"
statistics_buffer_memory_limit	number	2000000	Maximum size in bytes of statistics data buffered in Multiprotect service/daemon
mbss_stats_path	string	/data/mbss/stats/requestStats.gpb	Full path of statistics file of MBSS product
useTx2Protection	0 or 1	1	Do we take into account the TX2 licenses <div>NOTE</div> Available for TX2 board only, from v5.3.0
tx2LicensesPath	string	/usr/sbin/Multiprotect	Path of TX2 licenses file <i>mp_license_file</i> <div>NOTE</div> Available for TX2 board only, from v5.3.0
multiprotectLockPath	string	/var/run	Path of <i>multiprotect.lock</i> file <div>NOTE</div> For Linux only, from v5.3.0
default_scan_delay	number	6	Number of loops to scan a protection. A loop takes 5 sec. Default protection scan is 30 sec (6 x 5 sec). <div>NOTE</div> Added in v6.3.2

5.4) List of environment variables

Multiprotect License Protection also supports following environment variables

Variable	OS	Description	Default behavior if variable does not exist
LSDEFAULTDIR	Windows	Variable to identify where the software license file is located. NOTE You have to create a system environment variable (do not create a user environment variable) called <LSDEFAULTDIR> and set folder where license file will be copied (you must generally restart your computer to have this modification set). New folder must have enough read/write permission (SYSTEM permission) so that a license can be read/write by service called Multiprotect License Service	software license file is read from <code>C:\licences</code>
	Linux	NOTE You have to create a system environment variable called <LSDEFAULTDIR> This environment variable are located in <code>/etc/systemd/system/Multiprotect.service</code> file under Service section as <code>Environment=LSDEFAULTDIR="New folder"</code> , this New folder must have enough read/write permission (SYSTEM permission) so that a license can be read/write by service called Multiprotect License Service	software license file is read from <code>/usr/sbin/Multiprotect</code>
MP_CONF_DIR	Linux	Path of configuration files (for instance <code>slm_conf</code> , <code>app_conf</code>) NOTE From v5.3.0	configuration files are located in <code>/usr/sbin/Multiprotect</code>

6) How-To

6.1) How to Start/Stop/check Multiprotect License Protection service

6.1.1) Start/Stop/check Multiprotect License Protection service on Windows

If you want to start or stop Multiprotect, it can be done on 2 ways:

1. Go to Windows Services Panel (execute `services.msc`) and search for **Multiprotect License Service** to start/stop/restart Multiprotect.
2. Launch command prompt as administrator (`cmd.exe`) and type: `net start/stop "Multiprotect License Service"`

If you just want to check if service is running, go to `services.msc` and see its status.

6.1.2) Start/Stop/check Multiprotect License Protection service on Linux

You can start, stop or restart the server using these commands depending on your OS:

- OS supporting **systemd**, use `systemctl start/stop/restart Multiprotect.service`. (Multiprotect is the name of the service).
- OS supporting **init**, use `service mpld start/stop/restart`. (mpld is the name of the service).
- OS supporting **Upstart**, use `initctl start/stop/restart mpld`. (mpld is the name of the service).

You can check that Multiprotect is running by different ways depending on the distribution you are on.

- OS supporting **systemd**, use `systemctl status Multiprotect.service`.
- OS supporting **init.d**, use `service mpld status`.

6.2) How to know which Multiprotect version is installed?

6.2.1) Which Multiprotect version is installed on Windows?

You can see the version in the Multiprotect License Protection GUI and also via a command line: open a command prompt and execute the following commands:

```
cd C:\Program Files\Multiprotect
Multiprotect License Protection.exe -v
```

6.2.2) Which Multiprotect version is installed on Linux?

Execute the following command from a terminal:

```
/usr/sbin/Multiprotect License daemon -v
```


6.2.3) Which Multiprotect version is installed on Android?

Start License Manager app and go to settings > About

A pop-up will display version of the application.

6.3) How to reduce memory footprint?

By default, all types of protections are enabled in Multiprotect License Protection. If you have memory constraints, you can disable some protections (see list of parameters in §5.3).

For instance, if you want to enable only machine-locked (standalone) protection, you can disable all others protection types (hardware and network) as follow:

1/ please create a file *app_conf* with the following values:

```
useTOPS=0
useMTop=0
useMSO=0
useMorphoDongle=0
useSafenetDongle=0
useMepProtection=0
useTx2Protection=0
serverSoft=0
```

2/ restart Multiprotect License Manager service

6.4) How to enable logs?

1/ In the installation folder of Multiprotect License Manager, please create a file *app_conf* with the following values:

```
enableLog=1
logLevel=2
```

2/ Then restart Multiprotect License Manager service.

Log file *srv_trace_x.log* will be created in:

- Linux: */var/log/mp*
- Other environments: binary folder

6.5) How to manually register Multiprotect as a Windows service?

Needed only if you have installed Multiprotect License Protection version with "Copy only" option.

Procedure:

1/ Open a command prompt (*cmd.exe*) and move to the directory in which you installed the service. You should be logged as an Administrator or launch cmd as an Administrator.

2/ Install the service by executing the following command from the directory in which you installed the service: `Multiprotect_License_Protection.exe -i`

7) Troubleshooting

7.1) Standalone software license and firewire IEEE 1394 on Windows

If your PC has IEEE 1394 (firewire) interface and if you plan to use software standalone license, then to generate standalone software license for this computer, you have to:

- Disable FireWire (IEEE1394) interface (in device manager)
- Wait at least 30s and get ID of standalone software license (this id will not be dependent of your IEEE1394 interface)
- Then, enable your FireWire (IEEE 1394 interface)

If you do not disable IEEE1394 interface, then next time you reboot your computer, your license might not be valid anymore.

7.2) Standalone software license and bonding Ethernet interface

If you plan to use bonding Ethernet interface, we recommend you to lock your software standalone license to one of these two Ethernet card. Look at chapter 7.6.

7.3) Standalone software license with laptop computer

On some laptop computer, Ethernet interface is disabled if no cable is plugged. This could lead to change in you standalone software id. In energy saving panel (or in BIOS), disable automatic Ethernet interface disabling if no cable is plugged (could change from computer to computer)

7.4) Standalone software license on Linux and usb0 management console

If you have a management console on Linux using usb0 interface, we recommend you to perform same action that with FireWire 1394 on Windows.

- Disable usb0 interface (with command `ifconfig usb0 down`)
- Wait at least 30s and get ID of standalone software license (this id will not be dependent of your usb0 interface)
- Enable your usb0 interface (command `ifconfig usb0 up`)

If you do not disable usb0 interface, then next time you reboot your computer, your license might not be valid anymore.

7.5) Standalone software license and Virtual Machine

Standalone Software license is not compatible with Virtual Machine (VMWare, VirtualBox, etc.). If you plan to use standalone software license then you should use Multiprotect token server (see §2.2).

7.6) Software license with more than one Ethernet Card

To enable locking to multiple Ethernet card on a server computer, you have to:

- Create a file `app_conf`
- Add following line to `app_conf` file:
`lockMultipleCards=1`
- Restart daemon (restart using common daemon command or kill daemon)
or Windows Service (restart in Services Management window)

Then, if you have multiple Ethernet card (up to 6 supported), your id will have following format: `2010-xxxxxxxxxxxxxxxxxx`, `2010-xxxxxxxxxxxxxxxxxx` i.e. 2 standard id separated by a comma.

If one of these 2 ethernet cards is no longer available, then license will still be valid.

7.7) Software license have been installed successfully but is no longer valid

Please check your computer time. Set valid time on your computer and restart service.

7.8) Best practice for standalone license installation

Disable every elements which can have a MAC address and **keep only MAC address** you want to attach your license to.

Then,

- 1) Ask for generation
- 2) Install licenses
- 3) Enable every elements which have a MAC address

Your licenses will always be locked to your computer without any risk of license disappearing because locked to an invalid element.

7.9) hostID of software license has following format : 2004- *xxxxxxxxxxxxxxxxxx

If you have this kind of hostID, then your network is disabled. Enable at least one Ethernet interface.

7.10) Add software license success but did not see any license

First check your computer time and set a valid time if needed.

Then, if you are on a Virtual Machine (VM), standalone software license are not compatible on VM.

7.11) A software license which has been installed is not valid after a reboot

On many computers, we use some MAC address as a locking criterion. If MAC address which has been used for locking change, then previous license is not valid and another locking code is displayed.

To be sure to be locked to a fixed and immutable MAC address, disable every virtual device which can provide a MAC address and use this locking code.

This issue can also be linked with issues described in chapter 7.1 or 7.3

7.12) Cannot retrieve a network license from remote license server

If Multiprotect License Protection is configured to communicate with RMS token server, please check that your firewall does not block UDP port 5093. To do this test, you can temporarily disable your firewall if enabled and check if license retrieval succeed, then re-enable your firewall and add new rules to open this UDP port.

This issue can also occurs if configuration file has not been filled or if there is an error in configuration file. Check *app_conf* configuration file (see chapter 5.2.1).

7.13) Dongle protection is not working

Since Multiprotect License Protection v5.1.x, SafeNet dongle or MorphoDongle must be plugged before Multiprotect application starts.

In order to read a dongle protection, computer or Multiprotect service should be restarted.

7.14) Multiprotect service is consuming 100% of the CPU (rare case on Linux)

Multiprotect service is using **/tmp** folder to create pipe communication with others threads. If **/tmp/mp** and/or **/tmp/run** folders are cleaned-up, then Multiprotect service cannot work properly.

To prevent this, following exceptions are automatically added in *tmp.conf* file by Multiprotect installer:

```
# Add protection license exception
x /tmp/mp
```

```
x /tmp/run
```

If you are facing such problem, please check *tmp.conf* file and restart Multiprotect service.

NOTE

Depending on your OS, *tmp.conf* file is located as follows

/usr/lib/tmpfiles.d/tmp.conf, or **/run/tmpfiles.d/tmp.conf** or
/etc/tmpfiles.d/tmp.conf.

7.15) License is no more present on my Android phone

If after a while you notice license is no more present on my Android phone, there are 2 options:

- If there are more than 3 foreground services, Android OS will nominate the oldest service as a candidate for scavenging and termination. Please restart Multiprotect License Service application or restart your Android device and avoid having too many service in foreground
- Some phone manufacturers had set up a battery saving policy, which could move Multiprotect License Service in hibernation mode (for instance HUAWEI). In order to let manufacturer manager License Service's power manually, please go under Settings → Battery → Launch. Disable your automatic app power management and make it manual.

Sentinel® is a registered trademark of Thales, Inc.