

Working Directly With License Manager Configuration Files

License Manager configuration files can be modified using:

- >Sentinel Admin API (for all types of License Managers)
- >Sentinel Admin Control Center (for Admin API License Managers)

However, under certain circumstance it may be desirable or necessary to work directly with the configuration files using a text editor, as described in this section.

License Manager configuration files do not exist on a given machine until one or more of the following occur:

- >A user submits configuration changes in Admin Control Center.
- >The **writeconfig** command is issued in Admin API to write configuration changes to the configuration file.
- >A configuration file is created manually and placed on the machine.

Default Location of License Manager Configuration Files

This topic describes the location where each type of License Manager creates or expects to find its configuration file.

For all types of License Managers, this location can be determined in Admin API by retrieving the value of the configuration parameter **<configdir>**.

Admin License Manager

For the Admin LM on a given machine, the configuration file is called **hasplm.ini**. The pathname of the configuration file is as follows:

- >For Windows x64: *%CommonProgramFiles(x86)%\Aladdin Shared\HASP\hasplm.ini*
- >For Windows x86: *%CommonProgramFiles%\Aladdin Shared\HASP\hasplm.ini*
- >For Linux/Mac: */etc/hasplm/hasplm.ini*

The full path name of the **hasplm.ini** file is displayed in the Diagnostics report in Admin Control Center (see the **INI File** entry).

On a given machine, one **hasplm.ini** file exists for all software vendors who require the Admin LM on the machine.

NOTE If you are using Windows in a language other than English, locate the directory in which the common files are stored. (In English Windows, the *Common Files* folder).

Integrated/External License Manager

For the Integrated LM or External LM, the configuration file is called **hasp_vendorId.ini**. (*vendorId* is the Vendor ID associated with your Batch Code.) For each account under which a protected application executes on a given machine, the file is placed in one of the following locations:

Type of application	Default Location
Windows Desktop	<code>%LocalAppData%\SafeNet Sentinel\Sentinel LDK\</code>
Service (Local Service account) x64 operating system	<code>%systemroot%\SysWOW64\config\systemprofile\AppData\Local\SafeNet Sentinel\Sentinel LDK\</code>
Service (Local Service account) x86 operating system	<code>%systemroot%\System32\config\systemprofile\AppData\Local\SafeNet Sentinel\Sentinel LDK\</code>
Service (Network Service account)	<code>%systemroot%\ServiceProfiles\NetworkService\AppData\Local\SafeNet Sentinel\Sentinel LDK\</code>
Linux	<code>\$HOME/.hasplm</code>
Android	<p>The INI file should be in the .hasplm/ directory in the application data directory as returned by the Android <code>getFilesDir()</code> function.</p> <p>The value returned by this function is typically <code>/data/data/APP_NAME/files/</code> but the value could be different, depending on the Android version and installation.</p>

The Integrated/External LM also searches for configuration information from additional sources, in the following order:

1.(Windows only) The License Manager search for the **hasp_vendorld.ini** configuration file in the following locations:

- a.directory where the protected application is installed.
- b.the **%ProgramData%\Safenet Sentinel\Sentinel LDK** directory (for applications that were protected with Sentinel LDK 7.6 or later).

This file must be created and maintained manually.

If the **hasp_vendorld.ini** file is present in more than one of the locations described in this section, the License Manager merges the information in the files. Preference for conflicting information is given to files according to the following priority:

- a.default location
- b.application directory
- c.the **%ProgramData%\Safenet Sentinel\Sentinel LDK** directory

For example: If files are present in the default location and in the application directory, and both files contain a list of remote license server machines, the License Manager will search first for licenses in the list from the file in the default location. If the two files contain conflicting configuration information, preference is given to information from the file in the default location.

2.If the **Sentinel LDK License Manager** service on the local machine is active and “broadcastsearch” is enabled for the Integrated/External LM, the Integrated/External LM additionally uses the list of remote license server machines from the Admin LM.

NOTE An application that is linked with the Borland C static library (that is, *libhasp_windows_bcc_<vendorID>.lib*) does not access the Integrated/External License Manager configuration file. As a result, only default settings are used by the License Manager in this instance.

Modifying License Manager Configuration Files Manually

You have the option of creating a configuration file manually. This would be typically done when:

- >You want to distribute the same configuration parameters to many machines.
- >You want to place a configuration file in the application directory. A configuration file in this location would be shared by all users who run a protected application on a given machine.

The easiest way to create a configuration file is to copy an existing file that was created using one of the License Manager tools and modify it to suit your requirements.

The configuration file does not have to contain any parameters for which you accept the default values. A typical reason to create a configuration file manually is to specify a remote license server machine. In this case, the file would contain the following entry:

```
serveraddr = remoteServerAddress
```

This parameter is described below in greater detail.

For multiple entries, place each entry on a separate line in the file.

Additional License Manager Configuration Files Parameters

The table that follows describes configuration parameters that you can insert or modify in the configuration file for any type of License Manager (unless noted otherwise).

Parameter	Description
<code>disable_IPv6</code>	Whether to disable IPv6 protocol. Possible values are: 0 — Do not disable IPv6 protocol. Default. 1 — Disable IPv6 protocol.
<code>serveraddr</code>	Append specific machines that may be searched by the current machine for remote Sentinel License Managers. Specify data as IP addresses (for example: 10.1.1.17), Broadcast addresses (for example: 10.1.1.255), or machine names (for example: hklm001.ecomp.com). When using the IPv6 protocol, use the IPv6 address format. For example, specify FF02::1 to access all remote Sentinel License Managers that are part of the default local group defined in the IPv6 subnet.
<code>requestlog</code>	Whether to generate an access log file. Possible values are: 0 — Do not generate. Default. 1 — Generate.
<code>errorlog</code>	Whether to generate an error log file. Possible values are: 0 — Do not generate. Default. 1 — Generate.
<code>getinfo_uncached</code>	When the GetInfo function or GetSessionInfo function in the Sentinel Licensing API retrieves information about remote keys, the information may be obsolete by several minutes because of caching. (For example, the session/login counters may not be current for several minutes.) You can disable caching to deliver actual values. However, the additional network request requires significantly more time to retrieve.

Parameter	Description
	<p>Possible values are:</p> <p>0 — Enable caching. Default.</p> <p>1 — Disable caching.</p>
load_balancing	<p>Attempt to distribute licensing requests evenly by one of the following:</p> <p>server — Prefer remote License Managers with fewer sessions. Default</p> <p>container — Prefer remote keys with fewer sessions.</p> <p>none — No preference.</p> <p>Other priorities (license reuse, faster key preference, local key preference) always override these setting.</p>
broadcastsearch	<p>Whether to enable the current machine to search for remote Sentinel License Managers on the local network via broadcasts. (Note that the broadcast uses a random UDP source port. This may be an issue with certain firewalls.) If this option is not enabled, every machine on the local network that is to be searched must be specified with the serveraddr parameter (follows below).</p> <p>Possible values are:</p> <p>0 — Disable broadcasts.</p> <p>1 — Enable broadcasts. Default.</p>
emsurl	<p>The URL of a Sentinel LDK-EMS Service that is allowed to contact the Admin License Manager. This URL is only required on machines from which the user will access the Sentinel LDK-EMS Vendor Portal or Sentinel LDK-EMS Customer Portal.</p> <p>The default value is: <code>http://localhost:8080/ems</code></p> <p>However, if Sentinel LDK-EMS Service is located on a remote machine or if it uses a different port number, the URL must be changed accordingly.</p> <p>You can specify multiple emsurl parameters.</p>
port_admin	<p>You can restrict access to Sentinel Admin API and Sentinel Admin Control Center utilizing firewall restrictions. To implement this, specify any port other than 1947 or 80 for the port_admin parameter. For details, see Sentinel Admin API Reference.</p>

For example:

```

disable_IPv6 = 1
requestlog = 0
errorlog = 1
getinfo_uncached = 0
serveraddr = 10.1.1.17
serveraddr = 10.1.1.255

```

Additional License Manager Files

The table that follows describes additional directories and files that are created by the Admin License Manager under Windows.

The directories and files can be found under the following path:

>For Windows x64: *%CommonProgramFiles(x86)%\Aladdin Shared\HASP*

>For Windows x86, under *%CommonProgramFiles%\Aladdin Shared\HASP*

>For Linux/Mac: */var/hasplm/*

Directory	Content
attached	The Update/Attach function in Admin Control Center adds a copy of each V2C file that it processes to this directory.
detached	On a license server machine, the License Manager places a copy of each H2R file to this directory when a Detach License action is performed.
rehosted	When an SL key is rehosted from the current machine, a copy of the H2H file generated is placed in this directory.
cancelled	When a detached license is cancelled, a copy of the R2H file is placed in this directory on the recipient machine.
Imid	When Admin License Manager first detects the presence of License Managers on other machines within the same network, it automatically adds an ID file to this directory for each machine detected. The relevant ID file is used by the License Manager when a Detach License action is performed.

The files in the **attached**, **detached**, **rehosted**, and **cancelled** directories are used for logging purposes only. The user can delete these files if necessary.

The ID files in the **Imid** directory can be deleted. However, if the user later want to detach a license to one of the machines, they will have to manually create the ID file for the recipient machine (using Admin Control Center) and place the file in the **Imid** directory on the license server machine.