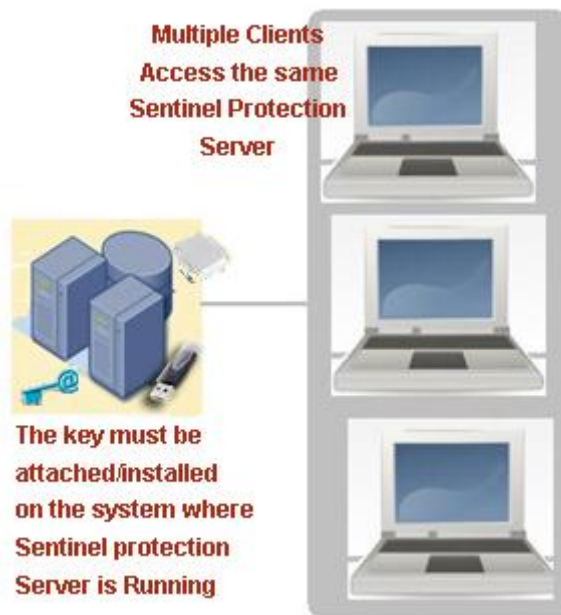


NETWORK LICENSE SENTINEL PROTECTION SERVER INSTALLATION GUIDE

1. The Photon Design Type D (Network) License

A Type D (Network) License allows you to access the software from more than one computer within the site, all these computers being connected to one computer network (Class C subnet).

The license is managed by plugging a USB or parallel port dongle into one of the computers of the subnet. In the guidelines below the computer on which the key is plugged will be called the server PC.



The network license will allow you to run as many copies of the software as you have licensed. If you start up more copies than you have licensed you will get a “key in use” error.

Notes:

1. You can only one run one instance of the application on each computer, even if you have free network user counts available.
2. The application PCs must be on the same Class C subnet (max 255 distinct addresses) as the license server PC (the computer hosting the key).
3. The PCs locate the license server by a broadcast message – any router on your network preventing broadcast messages from propagating will prevent the application PC from finding the license server.

2. Network Installation (Key Plug System)

If you have a network license you must install the **Sentinel Protection Server** on the server PC, where you intend to install the key. The server PC must be on the same subnet as the PCs wishing to use the application. No other setup is required to use the network license. The application PCs will find the server PC automatically.

2.1. Installing the driver and the Sentinel Protection Server

1. Go to the server PC and log in as administrator.
2. Run the keydriver\setup.exe from the installation disk, if you have not already done so via the program installation routine. Note that the key must not be plugged in during this process.

3. If Setup detects an older version of the Sentinel System Driver, you will be prompted to confirm the upgrade. The older version is uninstalled immediately after you confirm the upgrade. If you cancel out of the installation after this, you will not have your older version installed.
4. Select "custom" installation.
5. After you select "custom" you can choose whether to install parallel, USB, or both. Keep in mind that if your operating system does not support USB, the installer will not install it even if you select it.
6. Enable the install of the **Sentinel Protection Server**.
7. Disable the install of the **Sentinel Key Server** – it is not needed for our hardware keys.
8. Disable the install of the **Sentinel Security Runtime** - it is not needed for our hardware keys.
9. Continue on the installation and select "Install."
10. (USB only) If you have installed the keydriver as administrator then you must insert the key into the USB port before logging out of the account.
11. BIOS Parallel Port Setup. Some parallel port configurations can cause problems for the Key Plug drivers. To minimise the chance of problems, we recommend you reboot your machine and go into the BIOS settings to check the following:
 - a) (Win2K only) If you are running Windows 2000 please note the driver appears not work with a parallel port that is managed by Windows2000 using Plug and Play. If you have a Plug and Play BIOS, set your parallel port configuration to "BIOS managed" or "manual". Typically "Auto" settings will defer configuration of the port to the Windows2000 Plug and Play system, which causes problems in our experience.
 - b) Your BIOS will typically give you a choice of 2 or more of the following
 - ECP Mode
 - EPP Mode
 - Bidirectional Mode
 - Unidirectional Mode

We recommend you set to **ECP mode**, or if you do not have **ECP mode** then **unidirectional**. Save any BIOS settings changes and boot the machine into the Operating System.
12. Install Key:
 - (parallel port key) Plug the key into the parallel port of your computer. You can plug any printers into the other end of the key if you need to.
 - (USB key) Plug the USB key into your USB port or hub.
13. (Optional) You can check whether the driver is installed by running keydriver\medic\SentMed.exe from the installation CD.

2.2. Configuring the ports for the network license

You can choose the ports that the network dongle will use on the server PC; you should ensure that these ports are not being used by any other process (see Notes below).

The ports are controlled by a configuration file "sntlconfigsvr.xml", which is located in the Sentinel installation folder. In this file, the two lines used to configure the ports are:

```
<ConfigurePort>6001</ConfigurePort>
```

```
<ConfigureLicenseMonitorPort>6002</ConfigureLicenseMonitorPort>
```

In order to change the ports, simply replace "6001" and "6002" by the port of your choice and save the file.

Notes:

- The default location for the .xml file is "C:\Program Files\Common Files\SafeNet Sentinel\Sentinel Protection Server\WinNT".
- You will need to stop the Sentinel Protection Server in order to modify the configuration file. You can do so by selecting the Sentinel Protection Server in "Control Panel\System and Security\Administrative Tools\Services" and clicking on "Stop Service".
- You can check the status of a given port by running the command "netstat -a" in a Windows Command Prompt.

2.3. Creating usage and error logs for the network license

You can also set up this .xml file to keep a log of the license use and errors on the Server PC:

- The usage log records information related to the Sentinel Protection Server startup, shut-down, clients accessing the network keys and licenses in-use.
- The error log records errors related to network/client-server communication.

An example of syntax:

```
<LogUsages>C:/Temp/safenet_logusages.txt</LogUsages>
```

```
<LogErrors>C:/Temp/safenet_logerrors.txt</LogErrors>
```

If no path is selected then no logs will be generated.

The syntax used in the logs is described in section 3.

2.4. Using the Sentinel License Monitor

You can access the Sentinel License Monitor to check the status of the network license from anywhere on the subnet.

In a web browser, enter

<http://hostname:port/>

where hostname is the name of the server PC on the network and port is the license monitor port, by default 6002.

Note: from the server PC itself you can use <http://localhost:6002/>.

The “Sentinel License Monitor” will appear, displaying the number of keys connected to the host, the number of users (“Licenses-In-Use”) and the user limit for the key (“Hard Limit”).

Sentinel License Monitor - Windows Internet Explorer

System Address: <http://172.25.22.127:6002/>

Sentinel Protection Server Version 7.6.0

This web page shows you details of the keys attached/installed on the system.

Please click on a key number to view the details about the clients who are using the licenses available with this key.

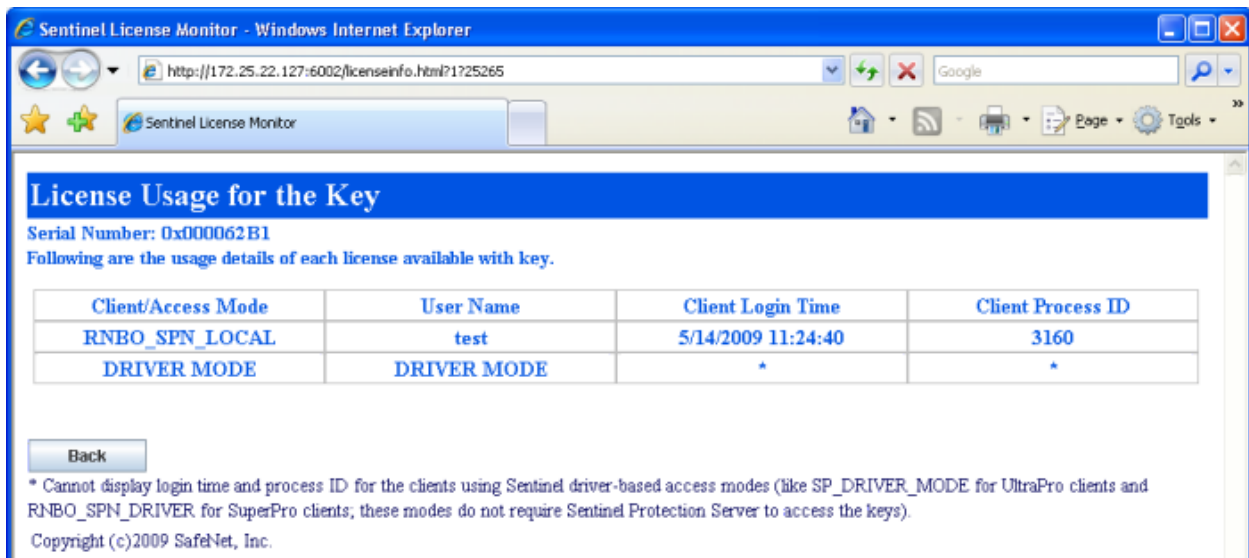
Keys#	Key Type	Form Factor	Serial Number	Model Number	Hard Limit	Licenses-In-Use	Highest Used	Time-Outs	Sublicense
1	SuperPro	USB	0x000062B1	*	1	0	0	0	>>
2	SuperPro	SOFT	0x00009057	*	1	0	0	0	>>
3	UltraPro	USB	0x00000013	UBJ00210	1	0	0	0	N/A

Refresh

* Not available. The model number cannot be obtained for certain keys. Please contact your developer/vendor for more information.

Copyright (c)2009 SafeNet, Inc.

By clicking on the key index below “Keys#” you can access the “License Usage for the Key”, displaying the computers from which the key is accessed and the corresponding user login.



2.5. Network license troubleshooting

If you obtain the error message:

- "027 error from key server: sorry, key not found" then the maximum number of allowed users has already been reached. Close the error message and check the Sentinel License Monitor to see where the software is being used.
- "028 error from key server: license in use" then there is already an instance of the software running on the server on a session that has been opened with your Windows user account. Close the error message and check the Sentinel License Monitor to see where the software is being used. This error may also occur if the program has not closed properly – please see below for further guidelines.

If you have trouble accessing the license, you can restart the Sentinel Protection Server without restarting your Server PC (admin rights needed). In order to do so:

- on the Server PC, go to Control Panel\System and Security\Administrative Tools\Services,
- in the list of services find "Sentinel Protection Server" and click on the "Restart" button.

If the program still fails to load, you can try and restart your computer.

Please note that you should find more information about the issue on the Server PC in Windows' "Event Viewer", which you can access from Control Panel\System and Security\Administrative Tools\Event Viewer. In the tree, select "Windows Logs/Application". You should obtain more information about the issue by looking for Error events associated with the Source "Sentinel Protection Server".

You can also check the usage and error logs of the Sentinel Protection Server if you have configured them.

2.6. Modifying or Uninstalling the Key Plug Drivers

1. Go to the Control Panel from the "Start" menu.
2. Select "Add/Remove Programs."
3. Look for the item that says "Sentinel System Driver" and select it.
4. The installer will allow you to modify, repair, or remove the installation, select which option you would like and follow along.
5. If you select modify, you can add in or remove the parallel or USB driver later.

2.7. Application Startup

When you start your application the program will initially look for a key via the Sentinel System Driver. If this fails it will check to see whether there is a **Sentinel Protection Server** running on the local machine with a key registered to the Server. This latter check is required for running a 32bit application on a 64bit OS.

If both these checks fail, then the application will look over your local network for a **Sentinel Protection Server**. Once it finds a key there may be a delay of up to 100s while it checks whether the key is in use by another copy of the application.

Please note that the start-up may also be delayed by up to 100s if the application did not close down properly the previous time.

If your application is using the Sentinel Protection Server and crashes, there will be a delay of 120s before the Sentinel Protection Server releases the license and you are able to start up the program – before this time the application will give the error 048 “license in use”.

3. Appendix: usages and errors logs syntax

The table below provides information about the transaction log file contents. For setting up of the log files please see section 2.3.

Code	Item	Description
1.	Version	Sentinel Protection Server version.
2.	Operation Code (any of the following)	The operation that took place.
	1 = issue license	A license is requested by the application/client.
	2 = release license	A request is sent to release the license.
	3 = time-out	Client's failure to update the Sentinel Protection Server.
	5 = startup	The Sentinel Protection Server started.
	6 = shutdown	The Sentinel Protection Server shutdown.
	8 = sublicense	A license is issued to a SuperPro client.
	10 = cancel license	A license is cancelled.
	16 = license request (no user limit)	A license is requested by a Sentinel SuperPro client (when the RNBOsproFindFirstUnit function is called and no user limit is provided).
3.	Time (in ticks)	System time in ticks, such as 1020336363.
4.	Time (as string)	System time as a string, such as: Tue Jan 01 00:00:01 2005.
5.	Key Index	Serial number of the key.
6.	Cell Number	Refers to the Toolkit Cell Address of the user limit programmed. A value "0" indicates that no user limit is being used.
7.	Host Name	The host name of the client machine.
8.	User Name	The user name of the client machine on the network.
9.	Client Process ID	The process ID of the client application.
10.	License Key	The hard limit of the key.
11.	License(s) in Use	The total number of licenses that are currently being used.
12.	Return Code	Operation return code.