

## Network Security Key (NP Series)

The NP series security key comes in either parallel (NP) or USB (NPU) format. In order for the security key to work with the operating system, you must install the Sentinel Protection Installer. A license server service called Sentinel Protection Server is installed on your system when you install the Sentinel Protection Installer. This service is necessary to manage network licensing of the network key. NOTE: Sentinel Protection Installer is only necessary for the license server and not necessary for the network client.

The installation of the Sentinel Protection installer is very straightforward. Sentinel Protection Installer is distributed as a self-contained executable. NOTE: if your security key is in USB format, you must unplug the USB key before installing the Sentinel Protection Installer. To install the Sentinel Protection Installer, you simply double-click on the Sentinel Protection Installer executable file and follow the instructions on screen during installation. IMPORTANT: you must login as administrator in order to install the Sentinel Protection Installer.

The Sentinel Protection Installer executable is located in the program CD under Sentinel Driver\Sentinel System Driver & Network License Server folder. The latest version of Sentinel Protection Installer is available for download from our web site at [www.integratedsoft.com](http://www.integratedsoft.com) under Support Useful Downloads

For more information, please see Sentinel Driver\SysAdminHelp\index.html located in the program CD.

## License Monitoring for NP Series Network Key

Sentinel License Monitor displays detailed information of the Sentinel keys attached to a system and the clients accessing them via a Web browser.

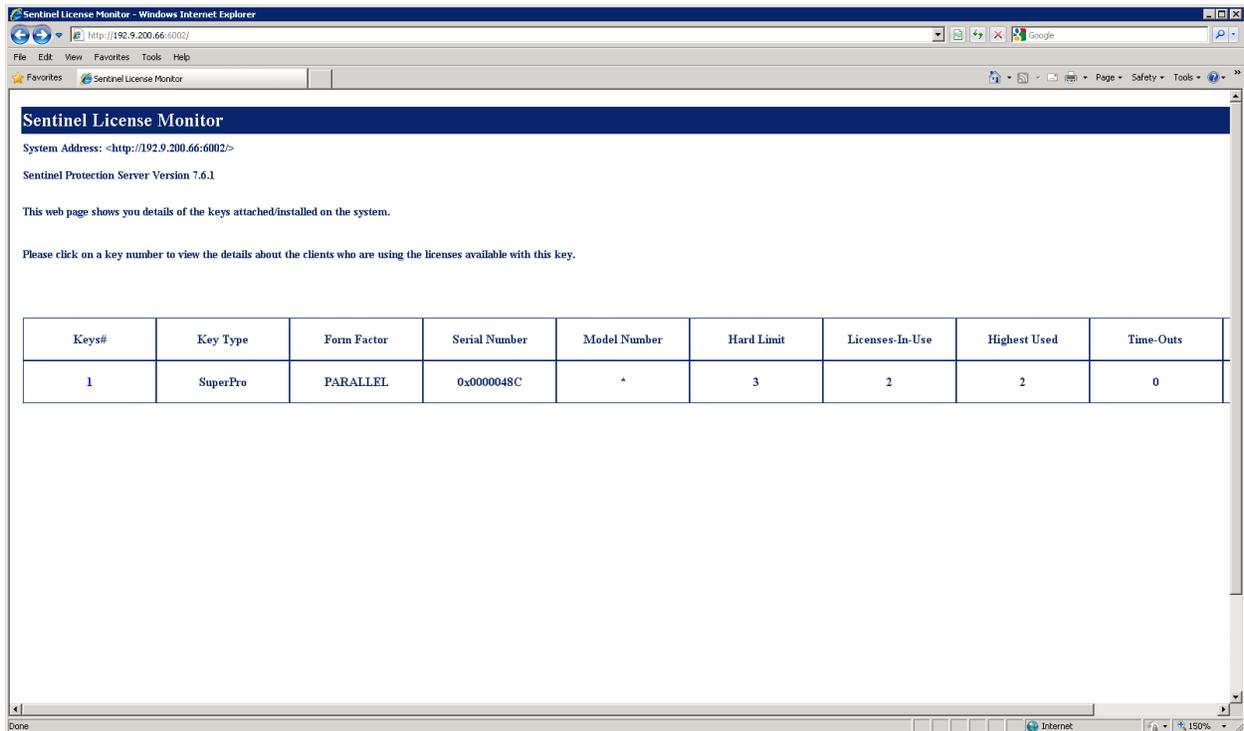
To launch Sentinel License Monitor, open web browser on the system. In the address bar, type the name or IP address of the system where the key is attached and Sentinel Protection Server is running in the following format:

http://IP address (or system name):HTTP port number

For example,

http://192.9.200.66:6002

Press the **Enter** key. The Sentinel License Monitor Web page is displayed.



Sentinel License Monitor

System Address: <http://192.9.200.66:6002/>

Sentinel Protection Server Version 7.6.1

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
1	SuperPro	PARALLEL	0x0000048C	*	3	2	2	0

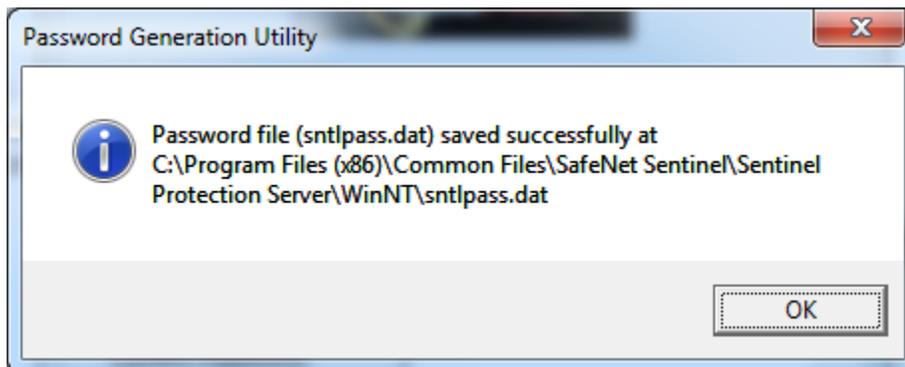
If desired, a system administrator or anyone with a password can cancel the licenses issued to the clients from a key. This situation might arise when the software is terminated abnormally without releasing its license.

Please follow the steps given below to enable the license canceling feature in the Sentinel License Monitor:

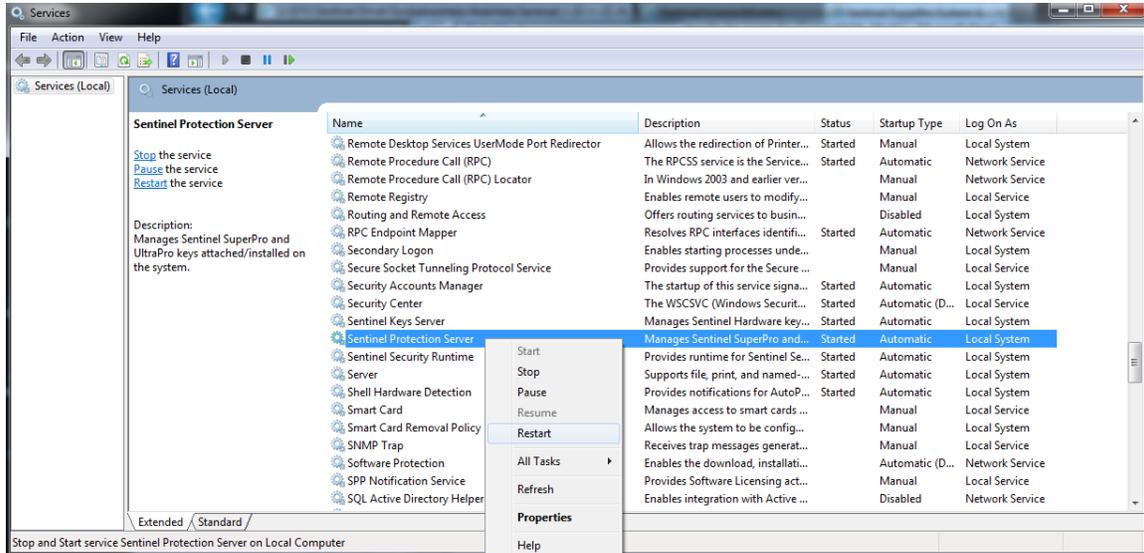
1. On the system where Sentinel Protection Server is installed, run the *PwdGenUtility.exe* to generate the *sntlpass.dat* file. The *PwdGenUtility* can be found at <OS Drive>:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel Protection Server\WinNT where <OS Drive> is the drive where the operating system is installed.



2. Click OK after you have entered your password. Do remember the password specified as it will be required for authenticating the license canceling request (see step 6).



- Restart the Sentinel Protection Server Service. To do this, go to Control Panel\System and Security\Administrative Tools\Services. Right click on “Sentinel Protection Server” and select “Restart” from the popup menu “.



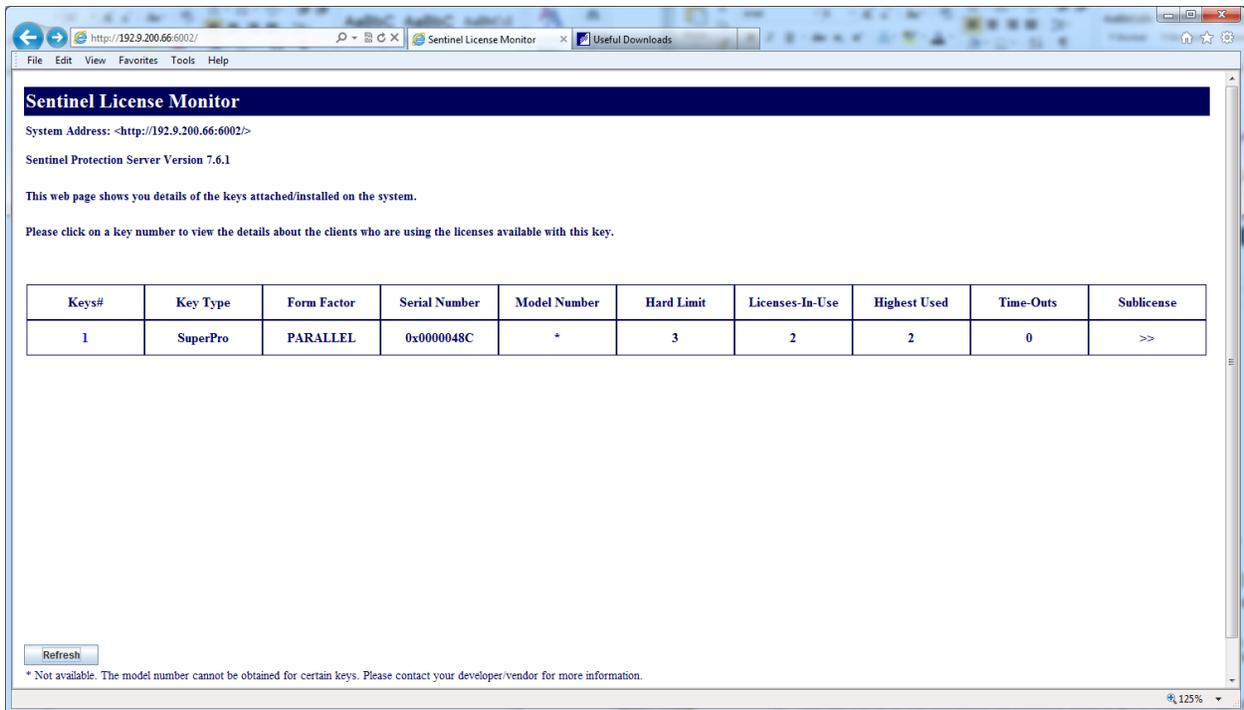
- Launch Sentinel License Monitor. Open web browser on the system. In the address bar, type the name or IP address of the system where the key is attached and Sentinel Protection Server is running in the following format:

http://IP address (or system name):HTTP port number

For example,

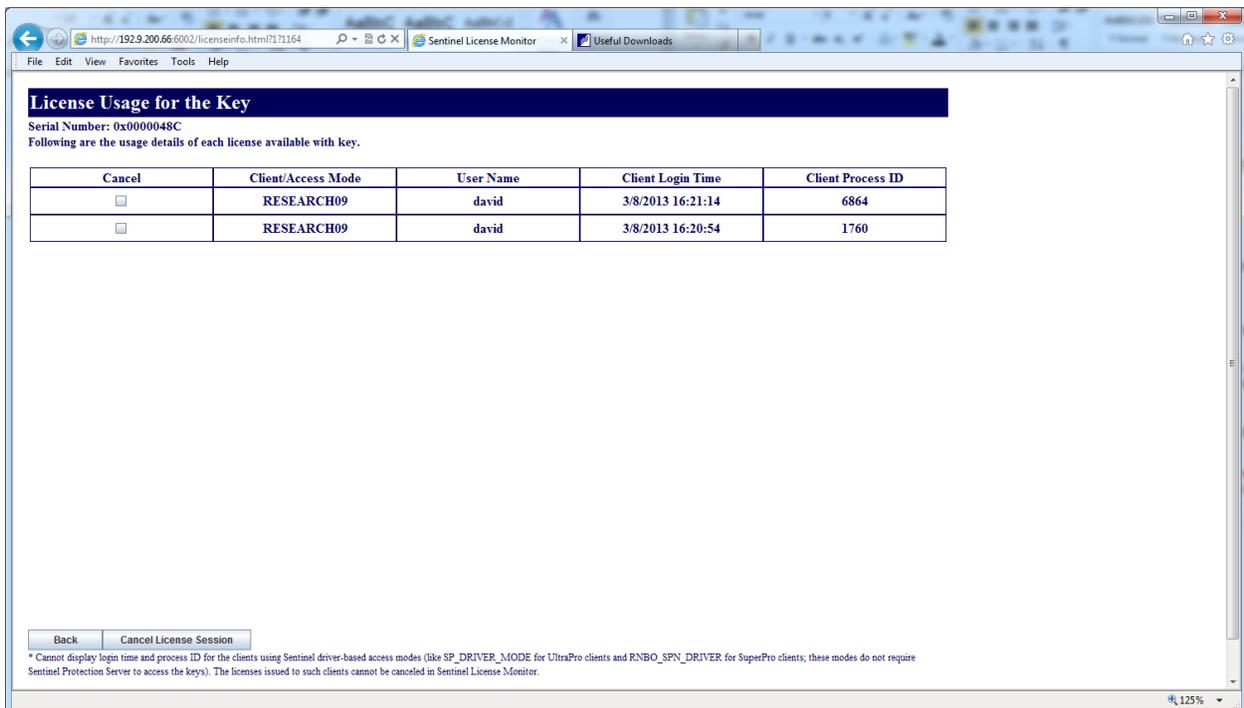
http://192.9.200.66:6002

Press the **Enter** key. The Sentinel License Monitor Web page is displayed. For example, in the Sentinel License Monitor screen below, the license sever with IP address 192.9.200.66 has one parallel network key with maximum of 3 users and 2 licenses are currently in use.

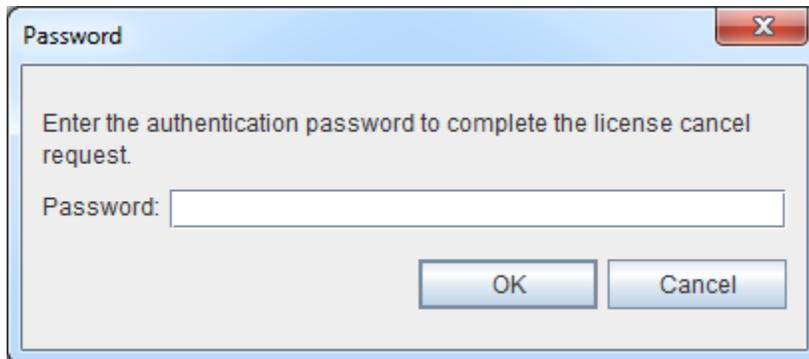


Click on the number under the Keys# column to select the key whose licenses are to be canceled. The license usage page will appear.

5. Select the **Cancel** check boxes for the licenses to be canceled. You can cancel up to 10 licenses at a time.



6. Click the **Cancel License Session** button given at the bottom of the page. A dialog box will appear prompting you to provide the same password specified in step 2.



7. Click **OK**. The key information page will appear.
8. You can verify for the license(s) canceled by launching the license usage page.

**NOTE:** The Sentinel License Monitor will not prompt you for any errors encountered while canceling a license. However, a license will not be canceled if there is excessive traffic in the network or you specified a wrong password in step 6.

For more information on how to setup Sentinel License Monitor, please see Sentinel Driver\SysAdminHelp\index.html locate in the program CD.

## Troubleshooting Network Key

There are two common problems running the network program.

1. If your license server is on a different subnet from your clients or if your program is taking excessive time to start, there is a workaround. You can specify your license server IP address when you start our software.

You can create a shortcut for the program executable. The program executable is located under C:\Program Files\IES\<program name> folder. Right click on executable file "IES.EXE" and select "Create shortcut" from the popup dialog. Once you have created a shortcut for "IES.EXE", right click the shortcut and select "Properties" from the popup dialog. Edit the "Target" box in the shortcut. Add the following program argument after IES.EXE:

```
-s xxx.xxx.xxx.xxx
```

where xxx.xxx.xxx.xxx is the IP address of the license server.

For more information, please follow the link below:

<http://www.integratedsoft.com/FAQ/General/Network-program-different-subnet>

2. A second but less common problem happens in a busy network. Our network program must periodically contact the license server to let the license server know that it is still "alive". If your network is busy, you may find your network program losing its license because it is unable to contact the license server in time. You can control the amount of time the license server is expected to hear from the client before declaring the client as "dead". The default period is 20 minutes. If the license server has not heard from the client during this period, the license is returned to the license server. You can create a shortcut for the program and edit the "Target" box in the shortcut. Add the following program argument after IES.EXE:

```
-t n
```

where n is a positive integer in multiple of 20 minutes. For example, n=6 is equal to 120 minutes.

For more information, please follow the link below:

<http://www.integratedsoft.com/FAQ/General/ServerTime-Out-Network-Key>

## Known Issues with NP Series Network Key

The network key and license server use UDP port 6001 for communication and broadcast. The License Monitor uses TCP port 6002 to monitor the license server. Both ports 6001 and 6002 must be open in order for the network key to work.

The following software has been known to conflict with our network key:

- National Instrument Software Lab View
- McAfee Intrusion Detection service

The most common issues are port contention and unopened or protected ports. Disabling the conflicting software and opening or enabling the ports should rectify the issues.

## Change ports used by Sentinel Protection Server and License Monitor

The default ports used by Sentinel Protection Server and License Monitor are UDP 6001 and TCP 6002 respectively. If disabling the conflicting software is not an option, Sentinel Protection Server and License Monitor can be configured to use different ports.

- 1) Find out port numbers already in use on your system. Open Command Prompt and type

```
Netstat -a -b
```

The port numbers that you pick should not appear in the Command Prompt. In this example, I will assume ports 8001 and 8002 are free to use.

- 2) Stop Sentinel Protection Server service. Go to Control Panel -> System and Security -> Administrative Tools -> Services. Right click on "Sentinel Protection Server" and select "Stop".
- 3) Edit C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel Protection Server\WinNT\Sntconfigsvr.xml

Look for

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

and

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

Change the "6001" to "8001" and "6002" to "8002". Save file and exit.

- 4) Restart Sentinel Protection Server service. Go to Control Panel -> System and Security -> Administrative Tools -> Services. Right click on "Sentinel Protection Server" and select "Start".
- 5) Edit sntlconfig.xml. Add "8001" between <ServerPort> tags.

```
<ServerPort> 8001 </ServerPort>
```

- 6) Copy sntlconfig.xml into the program folder (i.e. folder containing the executable IES.EXE).