Sentinel Protection Installer Version 7.6.9 (32-bit and 64-bit Windows) ReadMe

This ReadMe provides information about Sentinel™ Protection Installer, its installation and few tips on using the related components (such as, Sentinel License Monitor, Sentinel Protection Server, Sentinel Keys Server, Sentinel Keys License Monitor, and the driver configuration program).

Who Should Read This Document?

This ReadMe is for users who require Sentinel System Driver and/or Sentinel Security Runtime and/or Sentinel Protection Server and/or Sentinel Keys Server for accessing the Sentinel SuperPro, Sentinel UltraPro, or Sentinel Hardware Keys.

Note: Developers who wish to integrate these components in their Windows Installer-based setups should refer to the *Sentinel Protection Installer Help*.

Product Overview

The Sentinel Protection Installer is an integrated installer of the following components:

- **Sentinel System Driver**: The device driver for communicating with the following hardware keys:
  - Sentinel Hardware Key
  - Sentinel Dual Hardware Key
  - Sentinel UltraPro Key
  - Sentinel SuperPro Key
  - Sentinel Pro Key
- **Sentinel Security Runtime:** Sentinel Security Runtime is a program that provides runtime for the security of Sentinel SuperPro software keys (Secure Soft and Evaluation Soft) on a local machine.

- **Sentinel Keys Server**: The server component required for the network applications protected with Sentinel Hardware Keys.
- **Sentinel Protection Server**: The server component required for the network applications protected with Sentinel SuperPro or Sentinel UltraPro Keys.

Supported Component Versions

Sentinel Protection Installer 7.6.9 supports following versions of its components:

Component	Version Supported
Sentinel System Driver	7.6.0
Sentinel Security Runtime	1.0.1
Sentinel Protection Server	7.6.5.0
Sentinel Keys Server	1.3.6.0

Installation

This section contains details regarding the installation.

Platforms Supported

- This installer can be run on Microsoft Windows XP(32-bit and 64-bit), Server 2008 R2 (64-bit), Windows 7 (32-bit and 64-bit), Windows 8 (32-bit and 64-bit), Server 2012 (64-bit), Windows 8.1 (32-bit and 64-bit), Windows 10 (32 bit and 64-bit) and Windows Server 2016 (64-bit).
- The 32-bit Sentinel System Driver runs on Microsoft Windows XP (32-bit), Windows 7 (32-bit), Windows 8 (32-bit), Windows 8.1 (32-bit) and Windows 10 (32-bit). The 64-bit Sentinel System USB Driver runs on Windows XP (64-bit), Server 2008 R2 (64-bit), Windows 7 (64-bit), Windows 8 (64-bit), Server 2012 (64-bit), Windows 8.1 (64-bit), Windows 10 (64-bit) and Windows Server 2016 (64-bit).

  The 32-bit Sentinel System Parallel Driver runs on Microsoft Windows XP (32-bit), Windows 7 (32-bit), Windows 8 (32-bit) and Windows 8.1 (32-bit). The 64-bit Sentinel System Parallel Driver runs on Windows XP (64-bit), Server 2008 R2 (64-bit), Windows 7 (64-bit), Windows 8 (64-bit), Server 2012 (64-bit), and Windows 8.1 (64-bit).
- The 32-bit Sentinel Security Runtime runs on Microsoft Windows XP(32-bit and 64-bit), Server 2008 R2 (64-bit), Windows 7 (32-bit and 64-bit), Windows 8 (32-bit and 64-bit), Server 2012 (64-bit), Windows 8.1 (32-bit and 64-bit), Windows 10 (32 bit and 64-bit) and Windows Server 2016 (64-bit).
- The 32-bit Sentinel Protection Server runs on Microsoft Windows XP (32-bit and 64-bit), Server 2008 R2 (64-bit), Windows 7 (32-bit and 64-bit), Windows 8 (32-bit and 64-bit), Server 2012 (64-bit), Windows 8.1 (32-bit and 64-bit), Windows 10 (32 bit and 64-bit) and Windows Server 2016 (64-bit).
- The 32-bit Sentinel Keys Server is supported on Microsoft Windows XP (32-bit and 64-bit), Server 2008 R2 (64-bit), Windows 7 (32-bit and 64-bit), Windows 8 (32-bit and 64-bit), Server 2012 (64-bit), Windows 8.1 (32-bit and 64-bit), Windows 10 (32 bit and 64-bit) and Windows Server 2016 (64-bit).

Where Should I Run This Installer?

You must run this installer on the system where the hardware key is to be attached or the software key is to be installed. This can be a stand-alone system or a network system (where multiple applications in the subnet access the hardware keys concurrently).

Note: Internet installer does not include Windows installer 2.0

General Upgrade Information

The following point is useful if you are installing Sentinel Protection Installer for the first-time on a system:

- When you run the setup program, it will automatically update your version of the Windows Installer (to version 2.0) if necessary. It will not provide any prompt before doing this. If you are not sure you want to update the Windows Installer, do not run this program.

Note: Sentinel Security Runtime is upgraded automatically if its older version already exists on the system.

Installation Notes

Note: **Administrator privileges required for installing this software**
In order to set up this software on Windows NT-based platforms, you must have Administrator privileges.

Double-click the *setup.exe* provided with this product to launch the installer. Please follow the on-screen instructions to complete the installation.

The Installed Directory Structure

The Sentinel Protection Server, Sentinel Security Runtime, Sentinel Keys Server and the Sentinel System Driver files are installed at the locations explained in the table.

Note: **Do not move the files**
Do not move any of the files installed or the files that are created subsequently at these locations (such as the *sntlpass.dat* file which is generated for canceling a license).

Component	Path	Description
Sentinel System Driver	■ **On Windows 32-bit**: <OS Drive>\Program Files\Common Files\ Safenet Sentinel\Sentinel System Driver ■ **On Windows 64-bit**: <OS Drive>\Program Files(x86)\Common Files\ Safenet Sentinel\Sentinel System Driver	Contains *SetupSysDriver.exe* (the driver configuration program) and few driver-related files.
Sentinel Security Runtime	■ **On Windows 32-bit**: <OS Drive>\Program Files\Common Files\Safenet Sentinel\Sentinel Security Runtime ■ **On Windows 64-bit**: <OS Drive>\Program Files(x86)\Common Files\Safenet Sentinel\Sentinel Security Runtime	Contains the Sentinel Security Runtime's executable (*sntlsrtsrvr.exe*).
Sentinel Keys Server	■ **On Windows 32-bit**: <OS Drive>\Program Files\Common Files\Safenet Sentinel\Sentinel Keys Server ■ **On Windows 64-bit**: <OS Drive>\Program Files(x86)\Common Files\Safenet Sentinel\Sentinel Keys Server	Contains the Sentinel Keys Server's executable (*sntlkeyssrvr.exe)* that installs Sentinel Keys Server, the Password Generation Utility (PwdGenUtility.exe), the Sentinel Keys License Monitor files in the *\root* directory, and the files for cancel license module.
Sentinel Protection Server	■ **On Windows 32-bit**: <OS Drive>\Program Files\Common Files\SafeNet Sentinel\Sentinel Protection Server ■ **On Windows 64-bit**: <OS Drive>\Program Files(x86)\Common Files\SafeNet Sentinel\Sentinel Protection Server	■ The *\WinNT* directory is created, which contains the Sentinel Protection Server's executable (*spnsrvnt.exe*), the Password Generation Utility (PwdGenUtility.exe), the Sentinel License Monitor files in the *\root* directory, and the files for cancel license module ■ *loadserv.exe* ■ *SPNSrvStop.exe* ■ *SPNSrvSupport.exe*

Warning! Make sure that *\root* directory and its files of Sentinel Protection Server or Sentinel Keys Server are neither moved or deleted. This directory must co-exist with the Sentinel Protection Server or Sentinel Keys Server executable on a system.

Tips on Using Sentinel Protection Installer Components

This section contains tips on using the various applications and options that might be of help while you use Sentinel System Driver and/or Sentinel Protection Server and/or Sentinel Keys Server.

Sentinel Protection Server

About Sentinel License Monitor (For Sentinel UltraPro and Sentinel SuperPro Keys)

Sentinel License Monitor shows the details of the Sentinel UltraPro and Sentinel SuperPro keys attached/installed on a system and clients accessing them, via a Web browser. It is a convenient way to view and track the license activity and analyze application usage. You can use Sentinel License Monitor to perform the following tasks:

- View details about the keys connected to a system (such as, key type, form factor, serial number, model number and hard limit).
- Track how many licenses are currently in use.
- View the highest number of licenses issued by a key.
- Cancel the license issued to clients.
- Monitor the number of time-outs—the sessions that collapsed without properly releasing the license—recorded by the protection server for clients using licenses from a key.
- View the details of the client (such as, the user name, login time, and client process ID) who have currently obtained the license(s) from the key.
- View the details of the sublicense usage (such as, cell address, number in use, and limit) of a key.

Prerequisites for Launching the Sentinel License Monitor

Here are the specific requirements:

- Make sure that the Sentinel Protection Server is running on the system where the key is attached/installed.
- The client must have Javascript enabled in the browser.
- The client must be running Internet Explorer 7.0 (or higher)/Mozilla FireFox 47.0 (or higher)/Chrome/Edge.

Note: The parallel drivers are not installed by default. And customer need to explicitly select parallel drivers in the custom installation flow, in case he want to install parallel drivers.

Steps for Launching the Sentinel License Monitor

1. Open the Web browser on the system.
2. In the **Address Bar**, type the name or IP address of the system (where the key is attached/installed and protection server is running) in the following format:

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

For example,

```
http://172.25.22.127:6002
```

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

Sentinel License Monitor

Canceling a License

If desired, a system administrator can cancel the licenses issued to the clients from a key. This need might arise in situations when some other privileged client needs a license or an application terminates without releasing the license acquired.

Please follow the steps given below to cancel the licenses in the Sentinel License Monitor:

1. On the system where Sentinel Protection Server is installed, run the Password Generation utility (*PwdGenUtility.exe*) to generate the *sntlpass.dat* file. It is available at the following path:

   - **For Windows 32-bit**: *<OS drive>:\Program Files\Common Files\SafeNet Sentinel\Sentinel Protection Server\WinNT.*
   - **For Windows 64-bit**: *<OS drive>:\Program Files(x86)\Common Files\SafeNet Sentinel\Sentinel Protection Server\WinNT.*

Note: Do remember the password specified as it will be required for authenticating the cancel license request (see step 6).

2. Restart the Sentinel Protection Server.
3. Launch the Sentinel Licenses Monitor using the steps described in the “Steps for Launching the Sentinel License Monitor” on page 5. The key information page will appear.
4. Select the key whose licenses are to be canceled. The license usage page will appear.

5. Select the **Cancel** check box(es) for the licenses to be canceled. You can cancel up to 10 licenses at a time.
6. Click **Cancel License Session**. A dialog box will appear prompting you to provide the same password specified in step 1.
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: **Unable to cancel a license**
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.

About loadserv.exe

Using *loadserv.exe* you can:

- Install and remove the Sentinel Protection Server service.
- Set the server's log file locations. There are two separate log files, one for errors and one for processed transactions. If no locations are set for these log files, no logging will take place.
- Set the port used by the Sentinel Protection Server to launch the Sentinel License Monitor. You may need to do this in case the default HTTP port (6002) is being used by some other application.

About SPNSrvStop.exe

This utility is provided to stop the Sentinel Protection Server running on a Windows system.

About sntlconfigsrvr.xml (For Sentinel UltraPro and Sentinel SuperPro Keys)

Using *sntlconfigsrvr.xml*, you can configure the start-up settings for Sentinel Protection Server. This file helps you perform following:

- Define all the supported protocols from where the server accepts the client requests. The supported protocols is SP_TCP_PROTOCOL.
- Modify the server and client port for communication. You may need to do this in case the default client application communication port (6001) is being used by some other application.

Note: Modifying this port requires equivalent modification in client configuration file (*sntlconfig.xml*) too.

- Modify the Sentinel License Monitor port. The default HTTP port is 6002.
- Generate Client Request Response and error log files.
- Specify one or more IP address/IP address scope for the clients that are allowed or blocked.
- Set the time period in which the server will respond to client requests.
- Allow the server to cache the values of hardware key cells.

Note: Restart the Sentinel Protection Server to apply any changes you make to the server configuration file (*sntlconfigsrvr.xml*).

Sentinel Keys Server

About the Sentinel Keys License Monitor (For Sentinel Hardware Keys)

Sentinel Keys License Monitor shows the details of the Sentinel keys attached to a system and clients accessing them, via a Web browser. It is a convenient way to perform the following:

- View and track the license activity and analyze application usage. You can view the following details about the keys connected to a system:
  - Serial number, hardware key type, hard limit and licenses-in-use of the keys attached.
  - User limit and other details of the licenses used by a key.
  - Information about the clients (such as, the user name, login time, and client process ID) who have currently obtained licenses from the key.
- Cancel the current license sessions.
- View and configure the start-up settings for the Sentinel Keys Server, which are stored in the server configuration file **(***sntlconfigsrvr.xml*). Please see *page 13* for more information on *sntlconfigsrvr.xml* file.

Prerequisites for Launching the Sentinel Keys License Monitor

Here are the specific requirements:

- Make sure that the Sentinel Keys Server is running on the system where the key is attached/installed.
- The client must have Javascript enabled in the browser.
- The client must be running Internet Explorer 7.0 (or higher)/Mozilla FireFox 47.0 (or higher)/Chrome/Edge.

Note: The parallel drivers are not installed by default. And customer need to explicitly select parallel drivers in the custom installation flow, in case he want to install parallel drivers.

Steps for Launching the Sentinel Keys License Monitor

Note: By default, only the administrator of the local host (where Sentinel Keys Server is installed) can access "Configuration" page of Sentinel Keys License Monitor. If you are not the administrator of local host, make sure that your machine's IP address is added to the list of allowed users in sntlconfigsrvr.xml, before you access "Configuration" page of Sentinel Keys License Monitor.

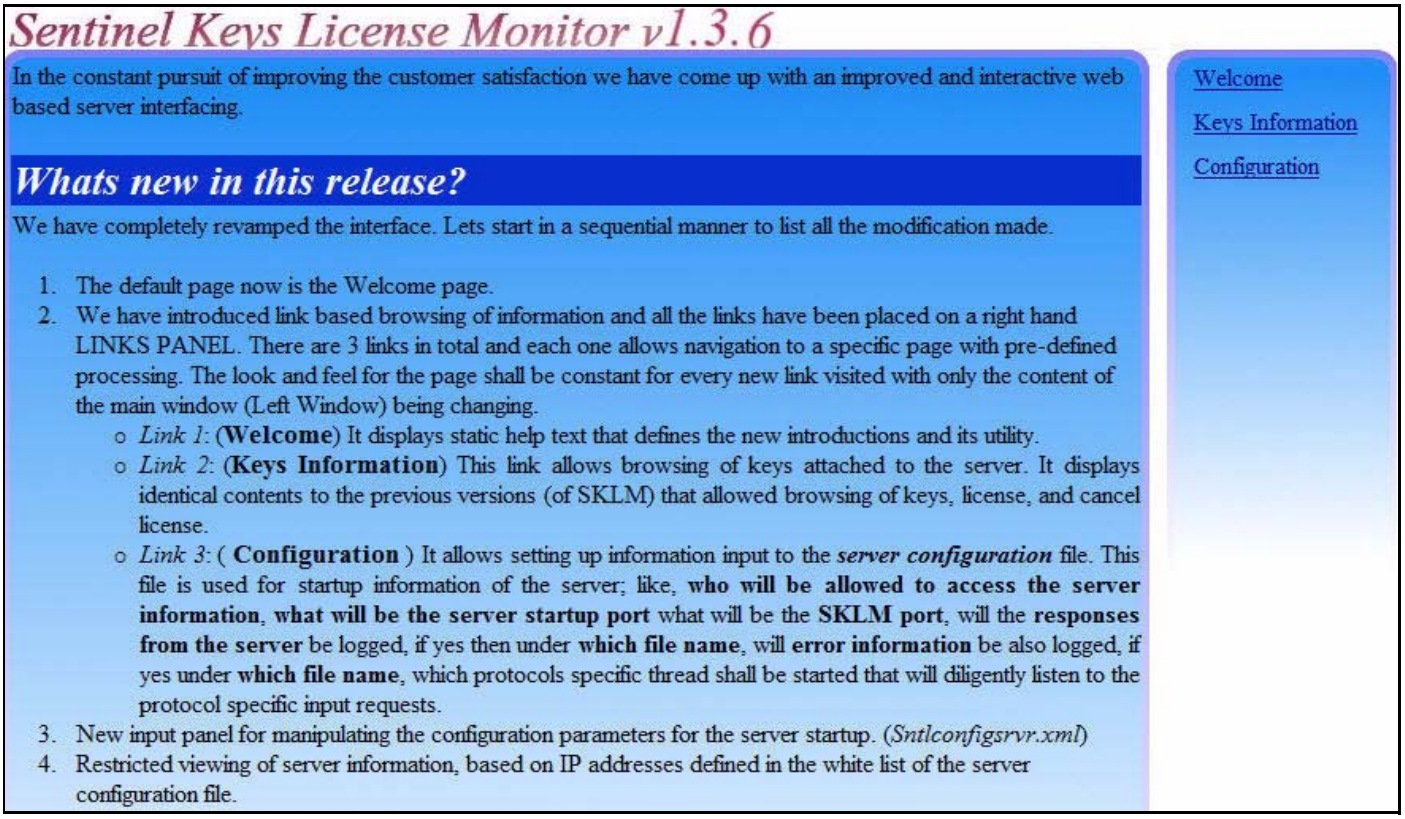
1. Open the Web browser on the system.
2. In the **Address Bar**, type the name or IP address of the system (where the hardware key is attached and Sentinel Keys Server is running) in the following format:

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

For example,

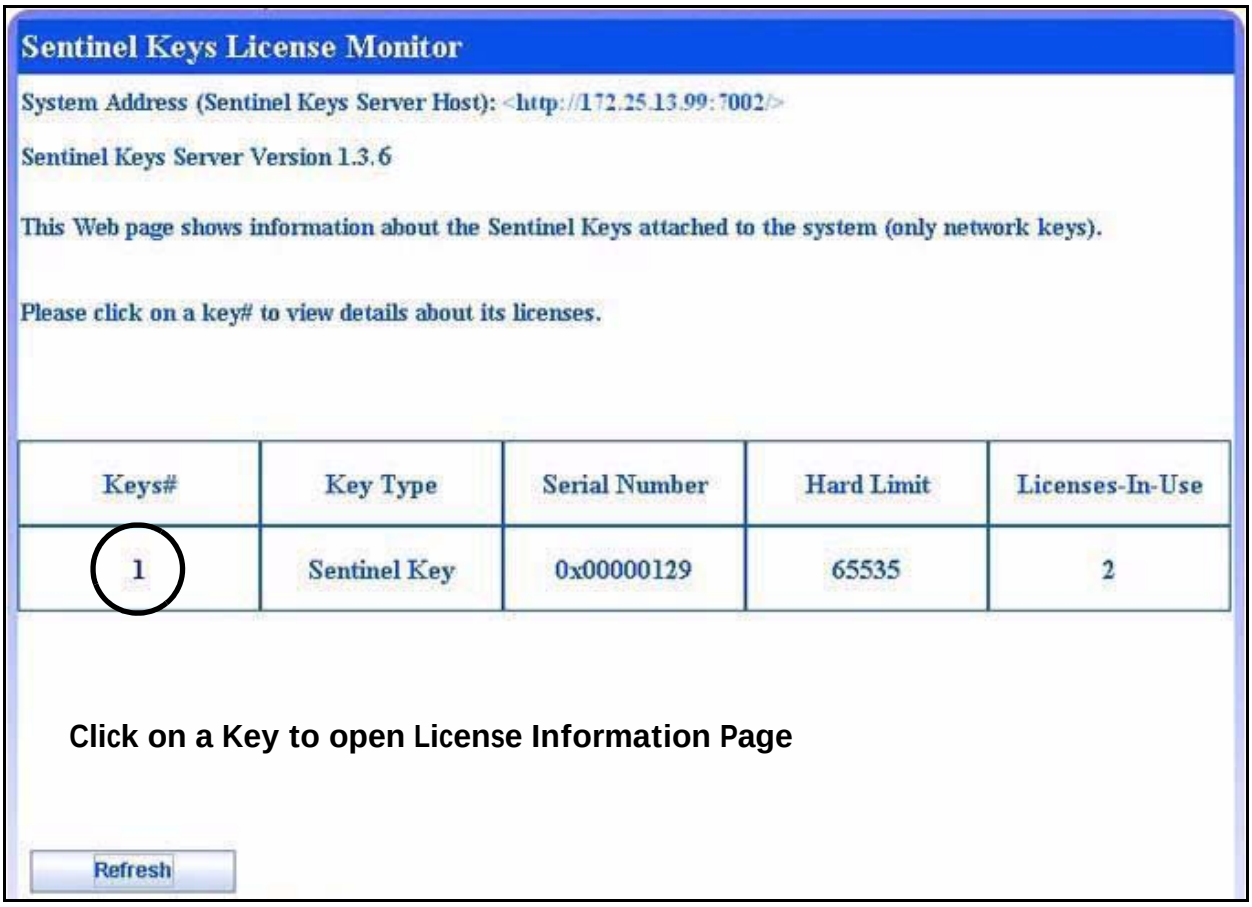
```
http://172.25.10.174:7002
```

3. Press the **Enter** key. The **Welcome Page** of Sentinel Keys License Monitor is displayed (if you are an allowed user of Sentinel Keys License Monitor, as shown below.

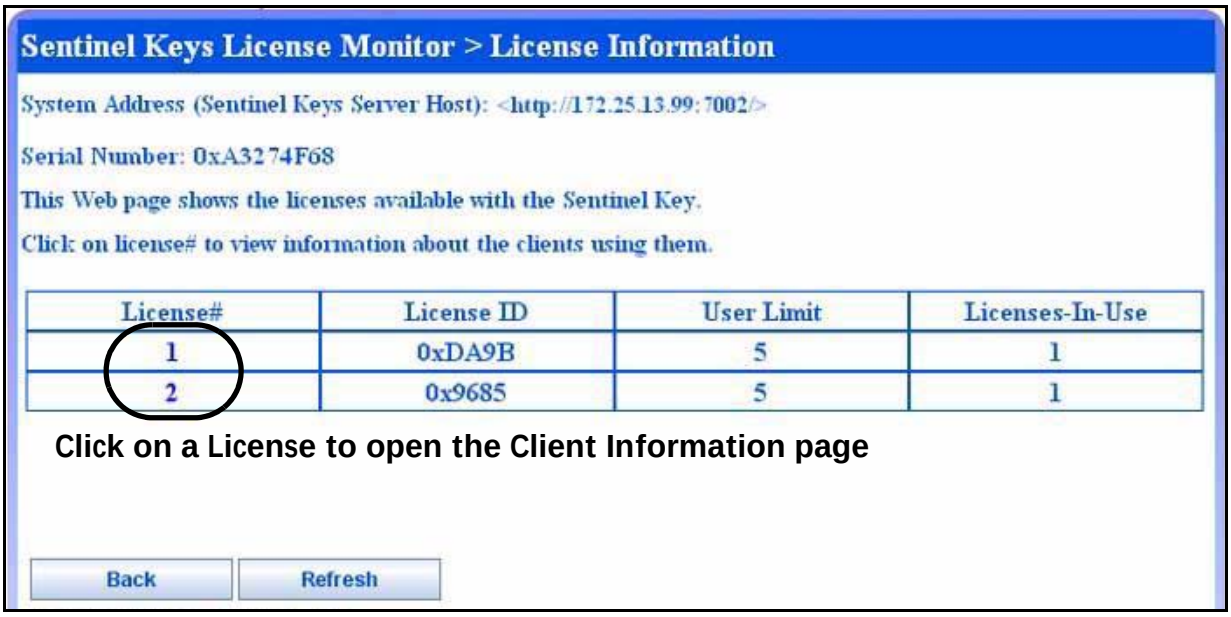


Sentinel Keys License Monitor - Welcome Page

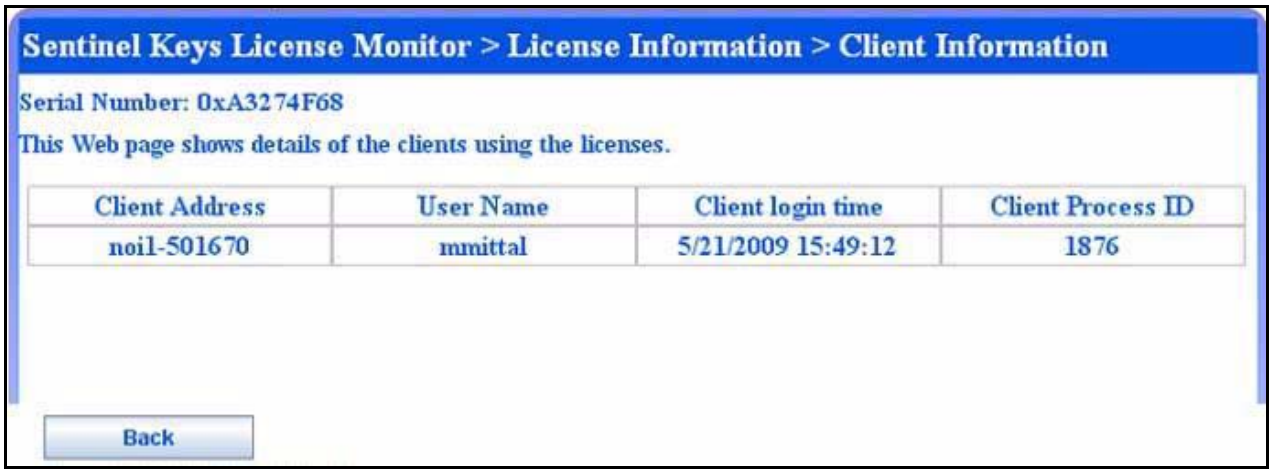
Navigation Options



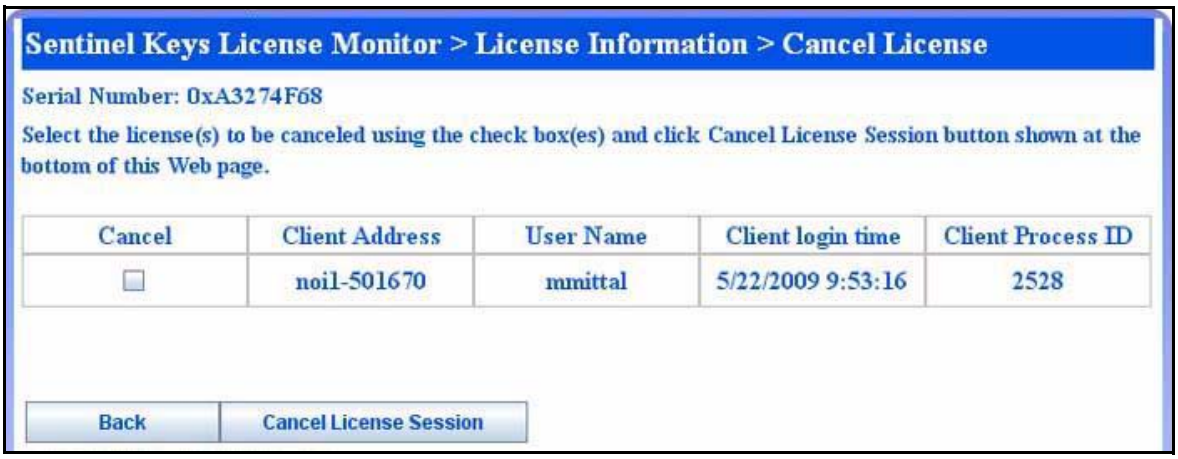
Sentinel Keys License Monitor - Key Information Page



Sentinel Keys License Monitor - License Information Page

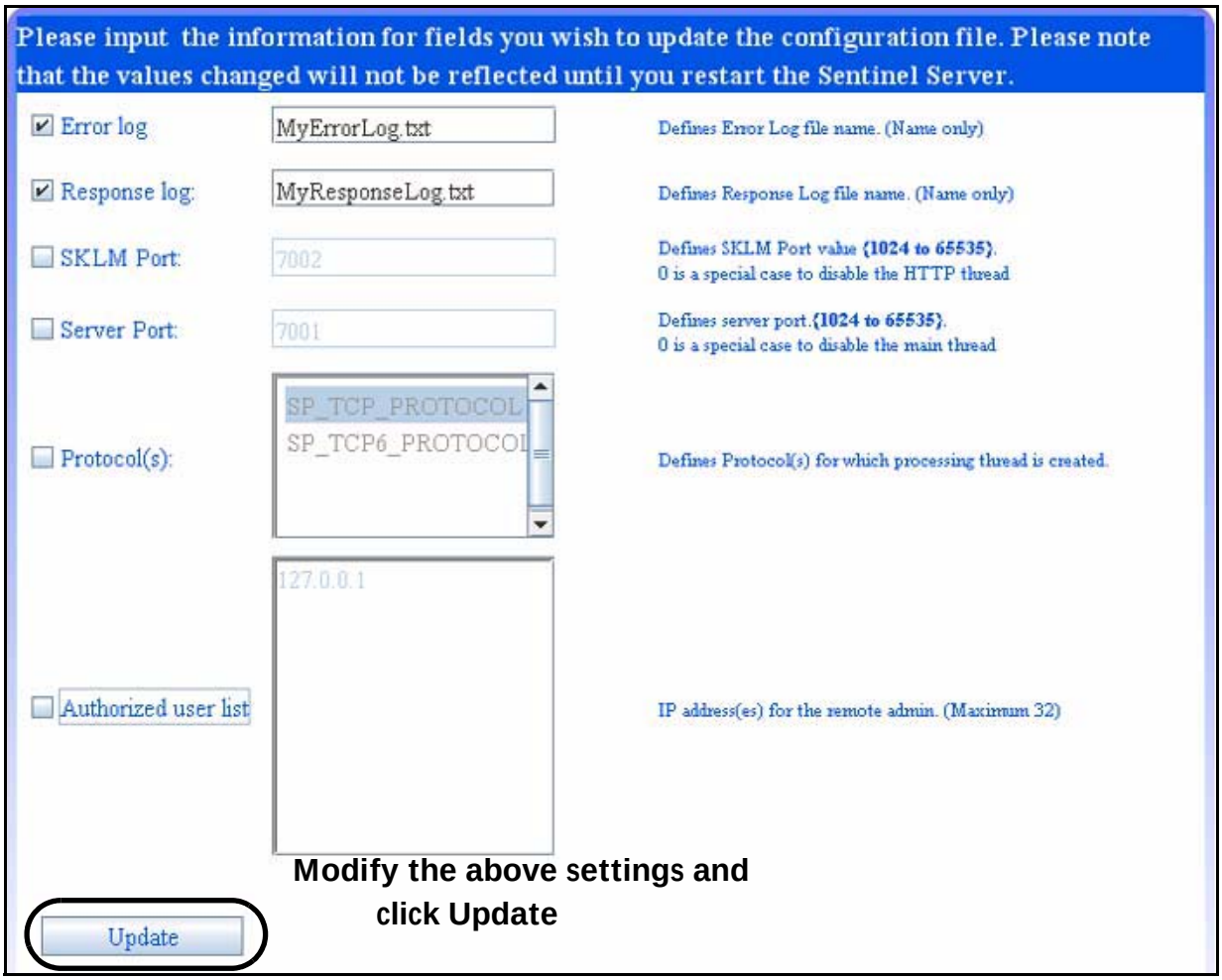


Client Information Page (When the Cancel License Option is Not Available)



Client Information Page (When the Cancel License Option is Available)

Note: To enable the cancel license option, make sure that the Password Generation utility is run to generate the *sntlpass.dat* file and the Sentinel Keys Server has been restarted.



Sentinel Keys License Monitor - Configuration Page

Note: The above page helps you configure the start-up settings for Sentinel Keys Server, which are stored in the *sntlconfigsrvr.xml* file. Please see *page 13* for more information on *sntlconfig-srvr.xml* file.

Canceling a License

If desired, a system administrator can cancel the licenses issued to the clients from a Sentinel Key. This need might arise in situations when some other privileged client needs a license or an application terminates without releasing the license acquired.

Please follow the steps given below to cancel the licenses in the Sentinel Keys License Monitor:

1. On the system where Sentinel Keys Server is installed, run the Password Generation utility (*PwdGenUtility.exe*) to generate the *sntlpass.dat* file. It is available at the following path:

   - **For Windows 32-bit:** *<OS drive>:\Program Files\Common Files\SafeNet Sentinel\Sentinel Keys Server*

Note: **For Windows 64-bit:** *<OS drive>:\Program Files(x86)\Common Files\SafeNet Sentinel\Sentinel Keys Server*Do remember the password; it will be required for authenticating the cancel license request (see step 8).

2. Restart the Sentinel Keys Server.
3. Launch the Sentinel Keys License Monitor. The main page (welcome) will appear
4. Click the **Keys Information** link in the navigation panel. The keys information page will appear.
5. Select the Sentinel Key whose licenses are to be canceled. The license information page will appear.
6. Select the license#. The client information page will appear.
7. Select the **Cancel** check box(es) for the licenses to be canceled. You can cancel up to 10 licenses at a time.
8. Click **Cancel License Session**. A dialog box will appear prompting you to provide the same password specified in step 1.
9. Click **OK**. Verify for the license(s) canceled.

The Sentinel Keys 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 8.

About sntlconfigsrvr.xml (For Sentinel Hardware Keys)

Using *sntlconfigsrvr.xml*, you can configure the start-up settings for Sentinel Keys Server. This file helps you perform following:

- Define all the supported protocols from where the server accepts the client requests. The supported protocols are SP_TCP_PROTOCOL (for TCP/IPv4) and SP_TCP6_PROTOCOL (for TCP/IPv6[1]).
- Modify the server and client port for communication. You may need to do this in case the default client application communication port (7001) is being used by some other application.

Note: Modifying this port requires equivalent modification in client configuration file (*sntlconfig.xml*) too.

- Modify the Sentinel Keys License Monitor port. The default HTTP port is 7002.
- Generate Client Request Response and error log files.
- Define the list of authorized users that are allowed to access Sentinel Keys License Monitor.

1. SHK supports TCP/IPv6 only on the same subnet. For a detailed list of operating systems for which SHK supports TCP/IPv6, please see *Release Notes* of SHK.

You can update the information stored in *sntlconfigsrvr.xml* by using the **Configuration** page of Sentinel Keys License Monitor. The **Configuration** page has been shown on page 12. To modify the settings, select the required check box(es) to enable the field(s), enter the required value, and click **Update**.

Note: Restart the Sentinel Keys Server to apply any changes you make to the server configuration file (*sntlconfigsrvr.xml*).

Sentinel System Driver

Using the Driver Configuration Program

Sentinel System Driver contains a configuration program called *SetupSysDriver.exe* to allow you configure the driver, if necessary. It also contains an option that allows you to call the original installer to modify, repair, or remove the installation.

The driver configuration program—*SetupSysDriver.exe*—is located at *<OS Drive>\Program Files\Common Files\SafeNet Sentinel\Sentinel System Driver* on 32-bit systems and located at *<OS Drive>\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel System Driver* on 64-bit systems. When you run it, a window will come up giving you a few configuration choices.

If you only have the USB driver installed, the configuration program will not detect the USB driver if no USB key is plugged in. This is because the plug-n-play USB driver is only loaded when a key is plugged in. This differs from the parallel driver, which is always loaded after it is installed, so the configuration program should always detect its presence.

Add/Repair/Remove Installation

If you select this option, the installer will run the Windows Installer and allow you to modify/repair/remove the installation. This option is the same as going to the **Add/Remove Programs** option.

Configure Driver

The **Configure Driver** option allows you to manually configure the parallel ports used by the Sentinel System Driver. In general, the driver is able to automatically detect your parallel ports and does not need to be set up manually. However, in some cases manual modifications are required. Any changes to the ports could potentially cause the driver to fail. For more information on changing the ports and various options, click the **Help** button.

Tip: **Sentinel System Driver automatically detects the user-configured, PCI parallel port cards**
A feature has been added to the Sentinel System Driver for Windows NT-based operating systems that will allow it to recognize add-in PCI parallel port adapters that have been configured by the operating system. You need not enter the port addresses assigned to those adapters.

Enable/Disable USB Driver Error Log

The **Enable USB Driver Error Log** button allows you to generate the error log files related to USB driver. If **Enable USB Driver Error Log** is selected and an error occurs with the USB driver while communicating with the key, the sntlusb.log file is created in the *<OS_Drive>*.

When clicked, the button toggles to **Disable USB Driver Error Log**, which you can select to disable generating the USB error log file.

Modify/Repair/Remove Instructions

If you have installed Sentinel Protection Installer using its *setup.exe* or the Sentinel Protection Installer's executable, then use the following instructions to repair/remove it.

For Windows NT-based Operating System

1. Open the Control Panel.
2. Double-click **Add/Remove Programs** to obtain a list of software programs installed on your system. Look for the Sentinel Protection Installer's entry.
3. Click **Remove** and follow the on-screen instructions. A message may appear asking you to reboot your system.

For Window Vista and Later

1. Open the Control Panel.
2. Under the **Programs** category, click **Uninstall a program**. The **Uninstall or change a program** window appears showing a list of the programs installed on your computer.

Note: If you are using the Classic View of the Control Panel, then double-click **Programs** and then double-click **Programs and Features**.

3. Select the Sentinel Protection Installer's entry and then click **Change**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

Getting Help

If you have questions, need additonal assistance, or encounter a problem, please contact Technical Support using the options provided below:

Contact Method	Contact Information
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA
Phone	United States: 1-800-545-6608
	International- 1-410-931-7520
Email	support@safenet-inc.com
Support and Downloads	www.safenet-inc.com/Support Provides access to the SafeNet Knowledge Base and quick downloads for various products.
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.

Copyright © 2017, SafeNet, Inc.
All rights reserved.

SafeNet, Sentinel, SuperPro, and UltraPro are either registered trademarks or trademarks of SafeNet, Inc. All other product names referenced herein are trademarks or registered trademarks of their respective manufacturers.

September 2017, Revision U