

Sentinel Keys Protection Installer (End User) - ReadMe

This ReadMe provides an overview of the Sentinel™ Keys Protection Installer, its installation and information about Sentinel Keys License Monitor, Sentinel System Driver, and Sentinel Keys Server.

Who Should Read This Document?

This ReadMe is for the application users (or their system administrators) who want to install the Sentinel System Driver and/or Sentinel Keys Server to access the hardware key.

Note: Windows-based 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 Keys Protection Installer is an integrated installer of the Sentinel System Driver¹ and Sentinel Keys Server².

The Sentinel System Driver is the device driver for communicating with the following USB hardware keys:

- Sentinel Keys
- Sentinel Dual Hardware Keys
- Sentinel UltraPro Keys
- Sentinel SuperPro Keys
- Sentinel Duo Keys (for SuperPro-protected applications on Macintosh)

For network applications protected using Sentinel Hardware Keys, Sentinel Keys Server is required.³

1. A daemon program for Linux and kernel extension module (KEXT) for Macintosh

2. A daemon program for Linux and Macintosh

3. For network applications protected using Sentinel UltraPro or SuperPro Keys, Sentinel Protection Server is required

Supported Component Versions

Sentinel Keys Protection Installer supports following versions of its components:

Component	Version Supported
Sentinel System Driver	7.5.1
Sentinel Keys Server	1.3.1

Installation

This section contains details regarding the installation.

Supported Platforms

On Linux

The following platforms are supported by the Sentinel System Driver and Sentinel Keys Server on Linux. Both run as daemon programs:

- ❑ Red Hat Enterprise Linux ES/AS 4.7 and 5.4 (32-bit and x64)
- ❑ Red Hat Enterprise Linux WS 4.7 and 5.4 (32-bit and x64)
- ❑ Red Hat Enterprise Linux Desktop 4.7 and 5.4 (32-bit and x64)
- ❑ Fedora 9.0 (32-bit and x64), 10.0 (32-bit), and 11.0 (32-bit)
- ❑ Open Suse 11.1 (32-bit and x64)
- ❑ Suse Linux Enterprise Server 10.2 (32-bit and x64)

On Macintosh

The following platforms are supported by the Sentinel System Driver and Sentinel Keys Server on Macintosh:

- Macintosh 10.3.9 (32-bit), 10.4.11 (32-bit), and 10.5.8 (32-bit) for PowerPC
- Macintosh 10.4.11 (32-bit), 10.5.8 (32-bit), and 10.6.1 (32-bit and x64) for Intel

If any application protected using the Sentinel products (listed below) is already installed on your system, this package will upgrade the existing Sentinel System Driver (KEXT/Framework). The upgraded Sentinel System Driver (version 7.5.1) is backward-compatible:

- Sentinel UltraPro
- Sentinel SuperPro
- Sentinel Keys Protection Installer

The Sentinel System Driver (KEXT) will be installed at: */System/Library/Extensions*. It will overwrite any previous installation of the Sentinel System Driver (KEXT).

Note: If you happen to install an earlier version of the Sentinel System Driver on your system after installing the latest Sentinel System Driver, no warnings will be shown to prevent overwriting of the latest Sentinel System Driver. For example, you may receive and install Sentinel SuperPro or UltraPro Keys from some other vendor after installing Sentinel Key-protected application. In such situations, you will face problem in accessing any or all of these hardware keys. To resolve this issue, you must reinstall the latest version of the Sentinel System Driver. A copy of which can be downloaded from: <http://www.safenet-inc.com/support/index.asp>.

Installation Notes

On Which System I Should Run This Installer?

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

You must have Administrator privileges (root user) in order to install this software.

For Linux

For installation on Linux, a script file and RPMs are provided. Run the *skpi_install.sh* script and choose your options accordingly.

Tip: You can use the *skpi_uninstall.sh* script to uninstall the program.

For Macintosh

Double-click the *SentinelKeysProtectionInstaller.pkg* provided to launch the installer. Please follow the on-screen instructions to complete the installation.

Before completing the installation, plug in the hardware key to load the Sentinel System Driver (KEXT). Else, restart the system after installation.

Note: The uninstallation script available with the Sentinel Keys Protection Installer (at: */Applications/SafeNet Sentinel/Sentinel Keys /<version>/Sentinel Keys Protection Installer/English/*) will uninstall both the Sentinel System Driver and Sentinel Keys Server.

Installed Components

Component Name	Installation Path
Sentinel System Driver	<ul style="list-style-type: none"> ❑ On Linux: <code>/opt/safenet_sentinel/common_files/sentinel_usb_daemon</code> ❑ On Macintosh: <code>/System/Library/Extensions/</code>
Sentinel Keys Server ^a	<ul style="list-style-type: none"> ❑ On Linux: <code>/opt/safenet_sentinel/common_files/sentinel_keys_server</code> ❑ On Macintosh: <code>/Applications/Safenet Sentinel/Common Files/Sentinel Keys Server</code>

- a. The Sentinel Keys Server installation also contains the files required for canceling licenses (using the Sentinel Keys License Monitor) and configuring the Sentinel Keys Server.

Important Information for Macintosh Users

If you have used the Sentinel Keys Protection Installer to install the Sentinel Keys Server, by default, the installer makes an entry in the system firewall to allow the socket communication—regardless of whether the system firewall is on or off.

However, on selected Macintosh platforms, this entry is not made automatically. You can use command line utility **plistbuddy** to make the corresponding server entry in firewall. This utility is present in `/Contents/Resources` folder of packages like **iTunes**.

However, on Macintosh systems that do not have **Plistbuddy** utility, this entry will not take place automatically. To create a new entry:

With your system Firewall enabled, make a new entry and add port numbers (Sentinel Keys Server uses 7001 and 7002 ports, by default) in *System Preferences/Sharing/Firewall* when running Mac OS 10.3.9/10.4.x, or in *System Preferences/Security/Firewall* when running Mac OS 10.5.x/10.6.1.

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 view and track the license activity and analyze application usage. 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-side configuration file (`sntlconfigsrvr.xml`).

Prerequisites for Launching the Sentinel Keys License Monitor

Here are the specific requirements:

- Sentinel Keys Server must be running on the system where the key is attached.
- The client must have Java Runtime Environment (JRE) 1.5 or higher.
- The client must be running Internet Explorer 6.0 (or higher)/ Netscape Navigator 4.6 (or higher)/Mozilla FireFox 1.0 (or higher)/Safari 1.3 (or higher)..
- The client must be added to the list of users that are allowed to access and use Sentinel Keys License Monitor. The IPv4 addresses of the allowed users are defined in the server-side configuration file, *sntlconfigsrvr.xml*. By default, only the administrator of the local host (where Sentinel Keys Server is installed) has the permission to access Sentinel Keys License Monitor. The administrator further adds IP addresses of machines that are allowed to use Sentinel Keys License Monitor.

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 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 Sentinel Keys License Monitor.

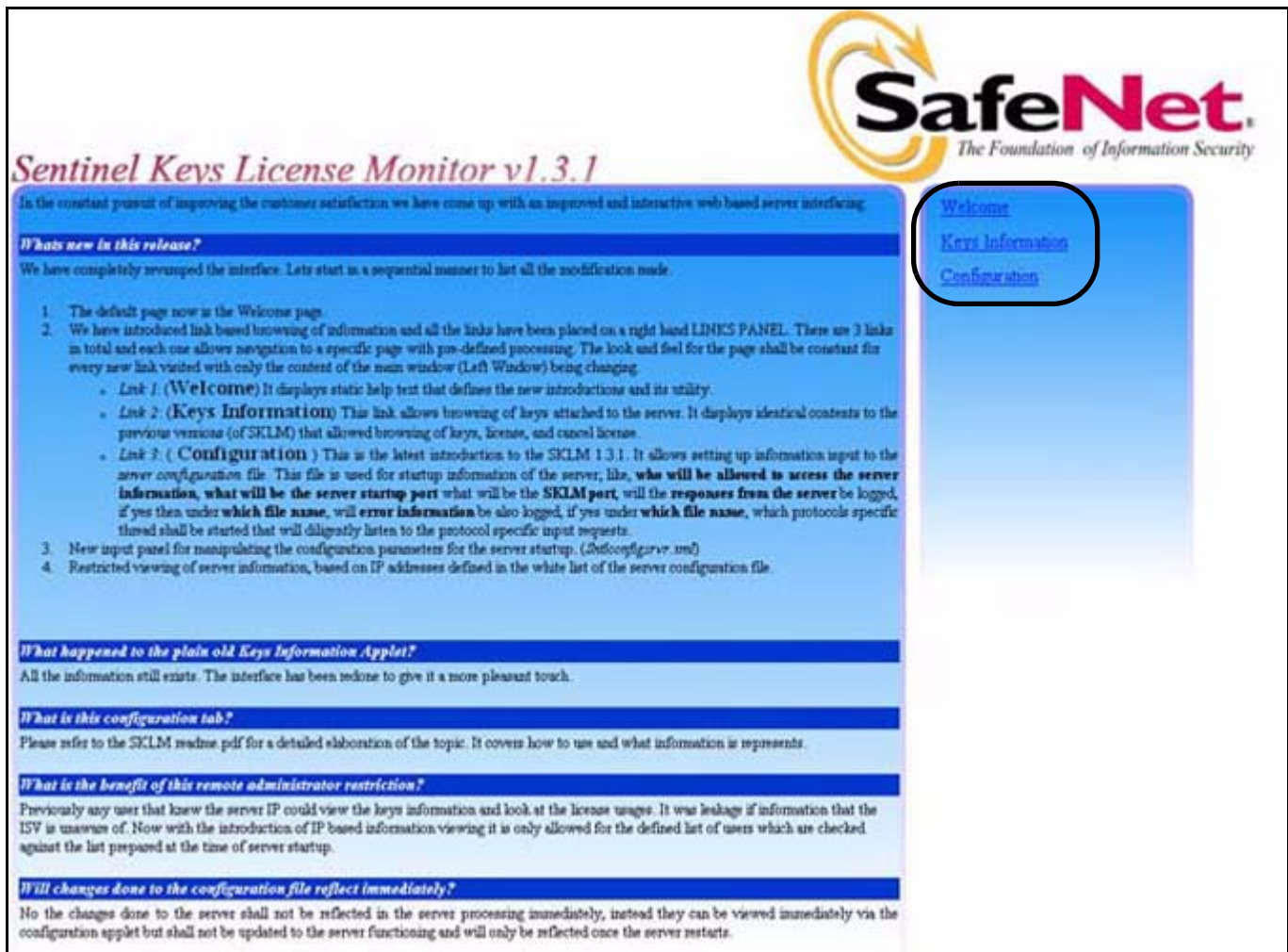
1. Open the Web browser on the system.
2. In the **Address Bar**, type the name or IP address of the system (where the hardware key is attached and Sentinel Keys Server is running) in the following format:

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

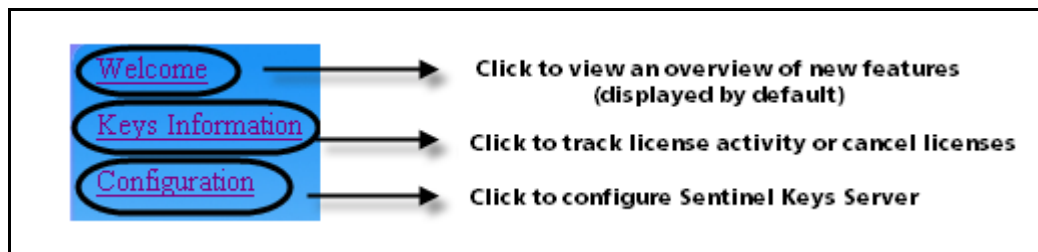
For example,

`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



Sentinel Keys License Monitor - Key Information Page

Sentinel Keys License Monitor

System Address (Sentinel Keys Server Host): <http://localhost:7002/>

Sentinel Keys Server Version 1.3.1

This Web page shows information about the Sentinel Keys attached to the system (only network keys).

Please click on a key# to view details about its licenses.

Keys#	Key Type	Serial Number	Hard Limit	Licenses-In-Use
1	Sentinel Key	0xA3274F68	5	2
2	Sentinel XM Key	0x3EDB3323	5	2

Click on a Key to open License Information Page

[Refresh](#)

Copyright (c) 2009 SafeNet, Inc.

Sentinel Keys License Monitor - Key Information Page

Sentinel Keys License Monitor > License Information

System Address (Sentinel Keys Server Host): <http://localhost:7002/>

Serial Number: 0xA3274F68

This Web page shows the licenses available with the Sentinel Key.

Click on license# to view information about the clients using them.

License#	License ID	User Limit	Licenses-In-Use
1	0xDA9B	5	1
2	0x9685	5	1

Click on a License to open the Client Information page

[Back](#) [Refresh](#)

Copyright (c) 2009 SafeNet, Inc.

Sentinel Keys License Monitor - License Information Page

Sentinel Keys License Monitor > License Information > Client Information

Serial Number: 0xA3274F68

This Web page shows details of the clients using the licenses.

Client Address	User Name	Client login time	Client Process ID
noil-501670	mmittal	9/21/2009 15:49:12	1876

Back

Copyright (c) 2009 SafeNet, Inc.

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

Sentinel Keys License Monitor > License Information > Cancel License

Serial Number: 0xA3274F68

Select the license(s) to be canceled using the check box(es) and click Cancel License Session button shown at the bottom of this Web page.

Cancel	Client Address	User Name	Client login time	Client Process ID
<input type="checkbox"/>	noil-501670	mmittal	9/22/2009 9:53:16	2528

Back

Cancel License Session

Copyright (c) 2009 SafeNet, Inc.

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.

Please input the information for fields you wish to update the configuration file. Please note that the values changed will not be reflected until you restart the Sentinel Server.

<input checked="" type="checkbox"/> Error log	<input type="text" value="MyErrorLog.txt"/>	Defines Error Log file name. (Name only)
<input checked="" type="checkbox"/> Response log	<input type="text" value="MyResponseLog.txt"/>	Defines Response Log file name. (Name only)
<input type="checkbox"/> SKLM Port	<input type="text" value="7002"/>	Defines SKLM Port value (1024 to 65535). 0 is a special case to disable the HTTP thread
<input type="checkbox"/> Server Port	<input type="text" value="7001"/>	Defines server port (1024 to 65535). 0 is a special case to disable the main thread
<input type="checkbox"/> Protocol(s):	<div><div>SP_TCP_PROTOCOL</div><div>SP_TCP6_PROTOCOL</div></div>	Defines Protocol(s) for which processing thread is created.
<input type="checkbox"/> Authorized user list	<div>127.0.0.1</div>	IP address(es) for the remote admin. (Maximum 32)

Modify the above settings and click Update

Sentinel Keys License Monitor - Configuration Page

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.

Note: Steps 1 and 2 are required only if the cancel license option is not enabled.

1. On the system where Sentinel Keys Server is installed, run the Password Generation utility⁴ to generate the *sntlpass.dat* file. It is available at the following path:
 - ❑ **For Linux:** */opt/safenet_sentinel/common_files/sentinel_keys_server*
 - ❑ **For Macintosh:** */Applications/Safenet Sentinel/Common Files/Sentinel Keys Server*
 Do remember the password; it will be required for authenticating the cancel license

4. The *PwdGenUtility.exe* for Windows and *PwdGenUtility* for Linux and Macintosh

- 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.

Note: 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.

Editing Server Configuration Information

1. On the Welcome page, click the **Configuration** link. The **Configuration** page is displayed as shown on page 9.
2. Select the check box(es) to enable the field(s) you want to edit, and enter the details as described below:
 - ☐ **Error log:** Specifies the name (not the path) of the log file, which is used to record errors related to network/client-server configuration.
 - ☐ **Response log:** Specifies the name (not the path) of the log file, which is used to record the transaction log for Sentinel Keys Server. It records information related to the Sentinel Keys Server startup, shut-down, clients accessing the network keys and licenses in-use.

Note: The specified file is created at the location where the Sentinel Keys Server is installed.

- ☐ **SKLM Port:** Sets the Sentinel Keys License Monitor HTTP port. The default port is 7002. It can be set as a value between 1024 to 65535. Setting it to zero (0) disables the SKLM port.
- ☐ **Server Port:** Sets the Sentinel Keys Server socket port. The default port is 7001. It can be set as a value between 1024 to 65535. Make sure that the port specified is not in use, and the same value is specified in the client-side configuration file. Setting it to zero (0) disables the Server port.

- ❑ **Protocol(s):** Sets the network protocol for the client-server communication. The supported protocols are SP_TCP_PROTOCOL (for TCP/IPv4) and SP_TCP6_PROTOCOL (for TCP/IPv6⁵).
 - ❑ **Authorized user list:** Specifies the IPv4 addresses of the remote clients that are allowed to access Sentinel Keys License Monitor. You can enter up to 32 valid IPv4 addresses.
3. Click **Update**. The *sntlconfigsrvr.xml* file is updated for the specified settings. However, you need to restart the Sentinel Keys Server for the updated settings to take effect.

Note: If multiple clients concurrently modify the *configuration.html* file, the XML file will reflect the last saved changes (the changes done by the user who is the last one to click **Update**).

5. SHK supports TCP/IPv6 only on the same subnet. For a detailed list of operating systems supported by TCP/IPv6, please see *Sentinel Hardware Keys Developer's Guide*.

Getting Help

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

Technical Support Contact Information

Customer Connection Center (C3)	
<i>http://c3.safenet-inc.com</i>	
Existing customers with a Customer Connection Center account can log in to manage incidents, get latest software upgrades and access the complete SafeNet Knowledge Base repository.	
Support and Downloads	
<i>http://www.safenet-inc.com/Support</i>	
Provides access to knowledge base and quick downloads for various products.	
E-mail-based Support	
support@safenet-inc.com	
Telephone-based Support	
United States	(800) 545-6608, (410) 931-7520
France	0825 341000
Germany	01803 7246269
United Kingdom	0870 7529200, +1 410 931-7520
Australia and New Zealand	+1 410 931-7520
China	(86) 10 8851 9191
India	+1 410 931-7520

Copyright © 2009, SafeNet, Inc.
All rights reserved.

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

November 2009, Revision G