

Sentinel Protection Installer Version 7.6.1 (Linux) ReadMe

This readme provides an overview of the Sentinel™ Protection Installer, its installation and a few tips on using the related components.

Who Should Read This Document?

This readme is for users who want to install the Sentinel System Driver and/or Sentinel Protection Server using the Sentinel Protection Installer setup program.

What is Sentinel Protection Installer?

The licensed application that you are using needs a few components to communicate with the Sentinel keys. The Sentinel Protection Installer is an integrated installer that installs these components in one-step on your computer. The components are:

- **Sentinel System Driver** – A daemon program for Linux which allows communication with the Sentinel USB keys.
- **Sentinel Protection Server** - A daemon program for Linux which manages licensing and security for the application you are using. The server must be run on the system where the Sentinel hardware key is attached.

Supported Component Versions

Sentinel Protection Installer 7.6.1 supports following versions of its components:

Component	Version Supported
Sentinel System Driver	7.5.4
Sentinel Protection Server	7.6.1

Upgrade Information

For Customers Using Sentinel SuperPro

- The Sentinel Protection Installer no longer supports Sentinel Parallel Port Driver.
- The *Sentinel UNIX Driver* has been now renamed as *Sentinel System Driver*.

Backward Compatibility

- Sentinel System Driver 7.5.1 is backward-compatible with the previous versions of Sentinel Protection Server, Sentinel keys, and application protected with the previous versions of Sentinel software. It supports the following USB hardware keys:
 - ☐ Sentinel Keys
 - ☐ Sentinel Dual Hardware Keys
 - ☐ Sentinel UltraPro Keys
 - ☐ Sentinel SuperPro Keys
- Sentinel Protection Server 7.6.1 is backward-compatible as well.

Installation

This section contains details regarding installation.

Supported Platforms

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

- Red Hat Enterprise Linux 5.11 (32-bit and x64), 6.6 (32-bit and x64), and 7.0 (x64)
- Fedora 20 and 21 (32-bit and x64)
- SUSE Linux Enterprise Server 11.3 (32-bit and x64) and 12 (x64)
- openSUSE 12.3 and 13.2 (32-bit and x64)
- Ubuntu 12.04 LTS and 14.04 LTS (32-bit and x64)*
- Debian 6.0 and 7 (32-bit and x64)*

** You need to install the Sentinel System Driver and Sentinel Protection Server separately on these platforms.*

Installation Notes

On Which System I Should Use This Installer?

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

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

Install Using Installation Script

Run the installation script using `sh protection_install.sh` command from the following location `/sentinel_protection_installer`.

Install Using the RPM Command

Install Sentinel USB Daemon

Use the `rpm -i sntl-sud-7.5.4-0.i386.rpm` command from the following location
`/sentinel_protection_installer/driver`.

Install Sentinel Protection Server

Use the `rpm -i sntl-server-7.6.1-0.i386.rpm` command from the following location
`/sentinel_protection_installer/server`.

For Users on Debian and Ubuntu Platforms

You need to install Sentinel USB Daemon and Sentinel Protection Server separately on Debian and Ubuntu platforms.

Install Sentinel USB Daemon

Run the installation script using `sh sud_install.sh` command from the following location:
`/sentinel_protection_installer/Debian_support/driver`.

Install Sentinel Protection Server

Use the `sh server_install.sh` command from the following location:
`/sentinel_protection_installer/Debian_support/server`.

Installed Components

Component	Installation Path
Sentinel System Driver	<code>/opt/safenet_sentinel/common_files/sentinel_usb_daemon</code>
Sentinel Protection Server*	<code>/opt/sentinel/sentinel_protection_server</code>

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

Tips on Using Various Options

This section contains tips on using the various applications and options that might be of help while you use Sentinel Protection Server:

About Sentinel License Monitor

Sentinel License Monitor shows the details of the Sentinel UltraPro and Sentinel SuperPro keys attached 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.

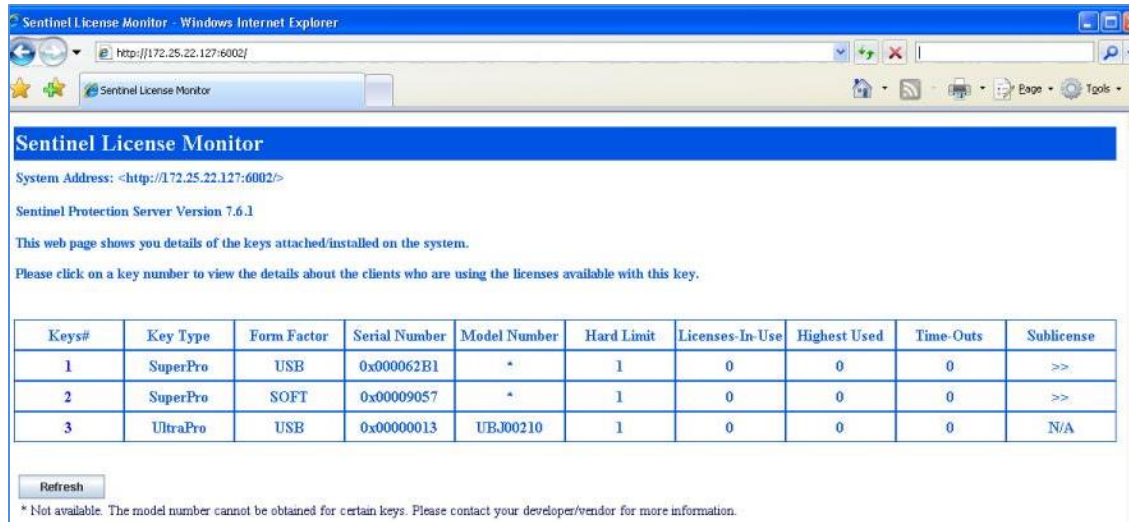
Prerequisites for Launching the Sentinel License Monitor

Here are the specific requirements:

- Make sure that the Sentinel Protection Server is running on the system where the key is attached.
- The client must have Java 2 Runtime Environment (JRE) 1.7.
- The client must be running Mozilla FireFox 3.6 and above.

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



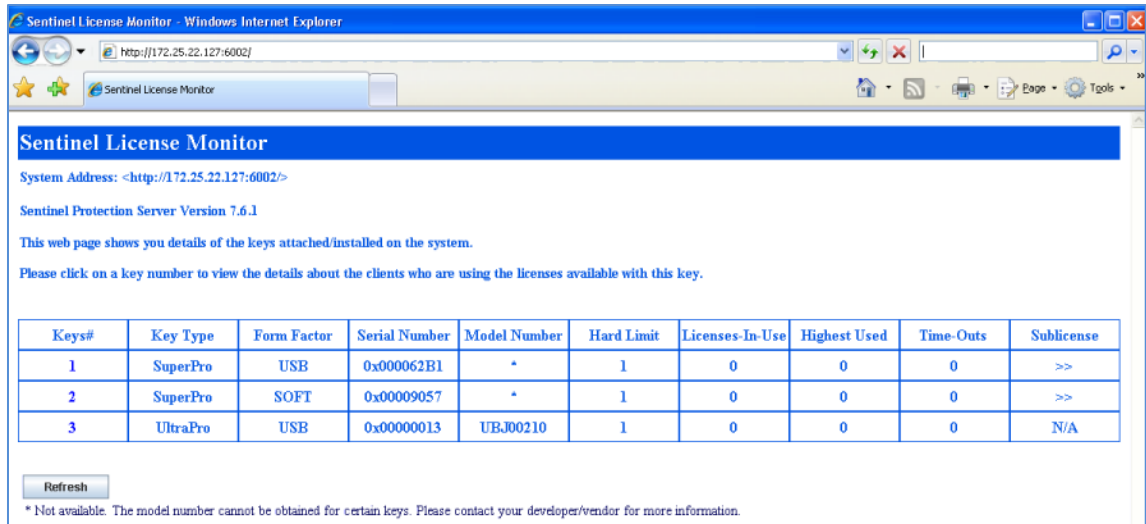
Sentinel License Monitor

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.

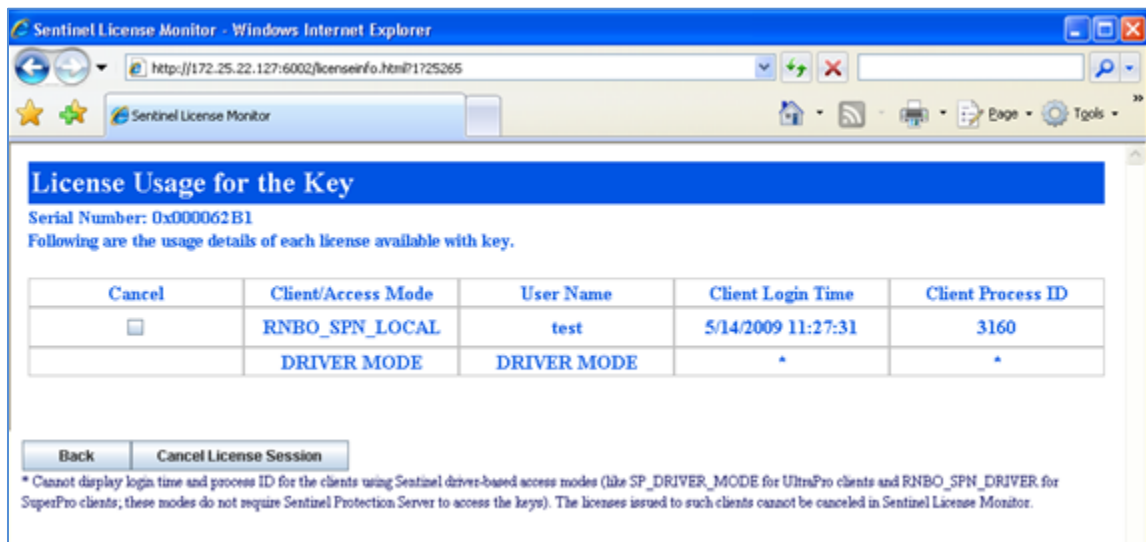
Please follow the steps given below to cancel the licenses in the Sentinel License Monitor:

1. On the system where Sentinel Protection Server is installed, run the *PasswordGenUtility* to generate the *sntl/pass.dat* file. 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.



The Key Information Page

4. Select the key whose licenses are to be canceled. The license usage page will appear.



The License Information Page

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 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 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

Using *loadserv* you can:

1. Stop the Sentinel Protection Server
2. Start the Sentinel Protection Server
3. Restart the Sentinel Protection Server
4. Query the status of Sentinel Protection Server

About sntlconfigsrvr.xml

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 protocol 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.

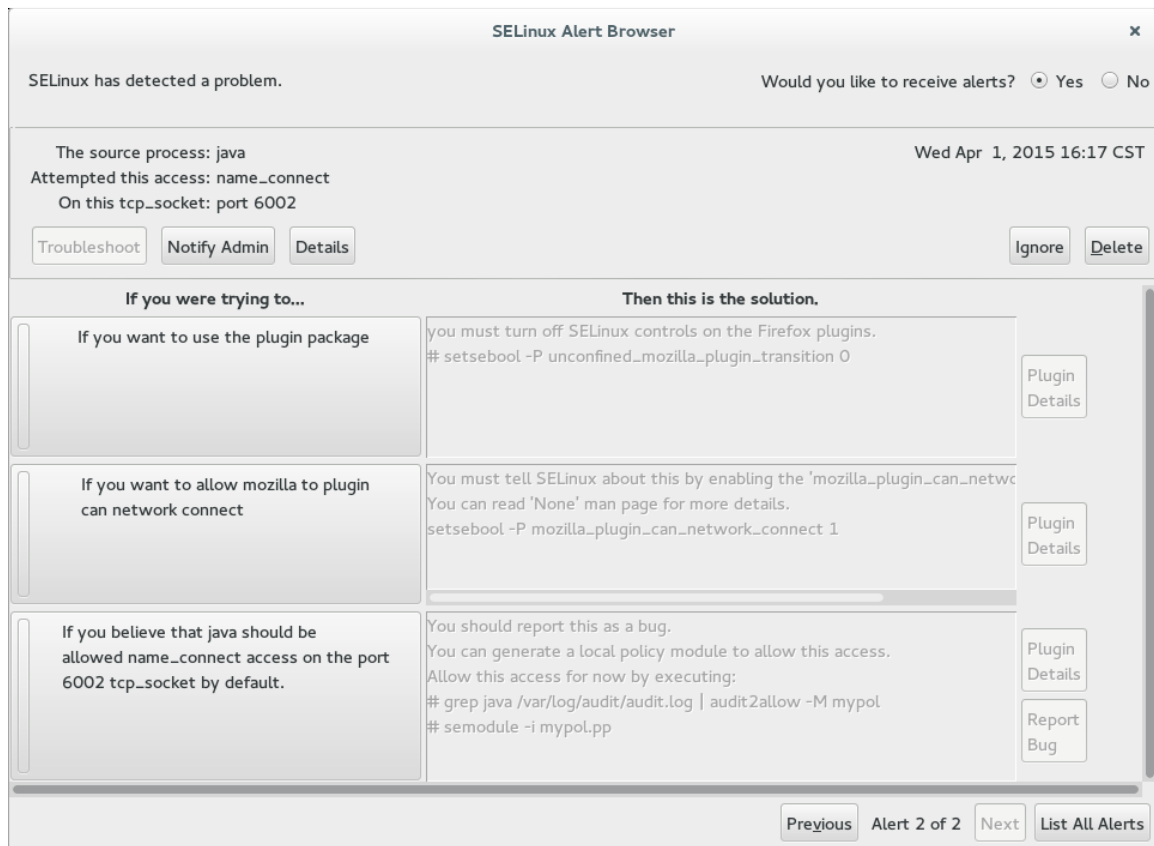
Note: Modifying this port requires equivalent modification in client configuration file (*sntlconfig.xml*) too.

- 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*).

Known Issue

SELinux prevents the execution of Java plugin while running Sentinel License Monitor, and throws the error message “SELinux Alert Browser” (AVC denial), as shown below:



To fix this issue, execute the following command as recommended by RedHat:

```
setsebool -P unconfined_mozilla_plugin_transition 0
```

Refer to the following link for more details:

https://bugzilla.redhat.com/show_bug.cgi?id=1141533

Getting Help

If you have questions, need additional assistance, or encounter a problem, please contact your software vendor.

Copyright 2015, SafeNet Inc.

All rights reserved.

<http://www.safenet-inc.com>

March 2015