

*System Administrator's
Guide*

SENTINEL SuperPro

 **RAINBOW**
T E C H N O L O G I E S

© Copyright 2000 – 2001, Rainbow Technologies, Inc.
All rights reserved.
<http://www.rainbow.com>

All attempts have been made to make the information in this document complete and accurate. Rainbow Technologies, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SentinelSuperPro is a trademark of Rainbow Technologies, Inc. Novell and NetWare are trademarks of Novell, Inc. Microsoft Windows, Microsoft Windows NT, Windows, Windows 95, Windows 98 and Windows 2000 are trademarks of Microsoft Corporation in the United States and other countries. All other product names referenced herein are trademarks or registered trademarks of their respective manufacturers.

Part Number 700663-001, Revision B
Software releases 6.1 and later

Revision	Action/Change	Date
A	Initial Release	October 2000
B	Updated server shut down and verification information	March 2001

RAINBOW TECHNOLOGIES, INC.

50 Technology Drive, Irvine, CA 92618
Telephone: (949) 450-7300, (800) 852-8569 Fax: (949) 450-7450

RAINBOW TECHNOLOGIES LTD.

4 The Forum, Hanworth Lane, Chertsey, Surrey KT16 9JX, United Kingdom
Telephone: (44) 1932 579200 Fax: (44) 1932 570743

RAINBOW TECHNOLOGIES

122, Avenue Charles de Gaulle, 92522 Neuilly-sur-Seine Cedex, France
Telephone: (33) 1 41 43 29 02 Fax: (33) 1 46 24 76 91

RAINBOW TECHNOLOGIES GMBH

Streiflacher Strasse 7, D-82110 Germering, Germany
Telephone: (49) 89 32 17 98 0 Fax: (49) 89 32 17 98 50

Additional offices are in the United States, Australia, China, India, the Netherlands, Russia and Taiwan. Distributors located worldwide.

Contents

Preface

Conventions Used in This Guide	vii
How to Get the Most from This Guide.....	viii
Getting Help.....	ix
<i>Using Online Help</i>	ix
We Welcome Your Comments	x

Chapter 1 – Getting Started

How Does a SentinelSuperPro-Protected Application Work?	2
<i>Stand-alone v. Network Applications</i>	2
<i>What Is a License?</i>	3
<i>What Is the SentinelSuperPro Server?</i>	5
<i>How an Application Obtains a Network License</i>	5
<i>What Is the SentinelSuperPro Monitoring Tool?</i>	7
What’s Included with the Protected Application?.....	8
SentinelSuperPro Software System Requirements.....	9
<i>Minimum Hardware Requirements</i>	9
<i>Minimum Software Requirements</i>	9

Chapter 2 – Installation

Where Should You Install the Server?	12
<i>Server Installation for Stand-alone Applications</i>	12
<i>Server Installation for Network Applications</i>	12
Where Should You Install the Protected Application?	13
SentinelSuperPro Software Installation Notes	14
Configuring the SentinelSuperPro Server Log Files	15

Contents

<i>Shutting down the Server in Windows NT or 2000</i>	<i>15</i>
<i>Setting the Log File Locations.....</i>	<i>16</i>
<i>Starting the Server</i>	<i>18</i>
Setting the Client Environment Variable.....	19
Installing the SentinelSuperPro Hardware Key	21
<i>Installing the Parallel Port Hardware Key</i>	<i>22</i>
<i>Installing the USB Hardware Key</i>	<i>23</i>
<i>Installing Keys after the Server Is Already Running</i>	<i>24</i>
Where to Go Next	25

Chapter 3 – Running the Protected Application

How the Application Locates a Key	28
<i>How a Stand-alone Application Locates a Key</i>	<i>28</i>
<i>How a Network Application Locates a Key</i>	<i>28</i>
How the Application Obtains a License.....	29
How the Application Maintains the License.....	30
When the Application Will Release the License	30

Chapter 4 – Using the Monitoring Tool

Starting the Monitoring Tool	32
Viewing Servers and Keys	33
<i>Viewing Server Information.....</i>	<i>33</i>
<i>Viewing Key Information.....</i>	<i>33</i>
<i>Searching for a Specific Server.....</i>	<i>34</i>
<i>Refreshing the Server List</i>	<i>35</i>
Viewing the Transaction and Error Log Files	36

Chapter 5 – Updating Your Keys

How Are Keys Updated?	38
<i>What Is a Locking Code?</i>	<i>39</i>
<i>What Is a License Code?.....</i>	<i>39</i>
Using Client Activator	40
<i>Client Activator System Requirements</i>	<i>40</i>
<i>Installing Client Activator.....</i>	<i>40</i>
<i>If You Aren't Using the Client Activator</i>	<i>41</i>

Using the Field Exchange Utility42

Installing the Field Exchange Utility42

Verifying the SentinelSuperPro Server Is Running43

Opening the Field Exchange Utility44

Generating a Locking Code44

Entering a License Code45

Appendix A – Glossary..... 47

Index 53

Preface

Welcome to the SentinelSuperPro system, which protects the application you are using. SentinelSuperPro may limit or meter application use, depending upon the unique requirements of your software license agreement.

Conventions Used in This Guide

Please note the following conventions concerning bold lettering, italics and more:

Convention	Meaning
Select	Use the arrow keys or mouse to select an item on a menu, a field in a window or an item in a list.
Click	Press the primary mouse button once. The primary mouse button is typically the left button, but may be reassigned to the right button.
Courier	Denotes syntax, prompts and code examples. If bold, denotes text you type.
Bold Lettering	In procedures, words in boldface type represent keystrokes, menu items, window names or mouse commands.
<i>Italic Lettering</i>	Words in italics represent file names and directories, or, when used in explanatory text, for emphasis.

How to Get the Most from This Guide

The *SentinelSuperPro 6.1 System Administrator's Guide* walks you through the entire process of installing the protected application(s) and SentinelSuperPro software, including information on configuring the client, running the protected application and monitoring license usage. The following table explains what you can find in each chapter of this guide:

Chapter/Appendix	Description
Chapter 1 – Getting Started	An overview of how the protected application uses SentinelSuperPro, and how the protected application will run on your network.
Chapter 2 – Installation	Information about installing the SentinelSuperPro software, configuring the client and server and installing the hardware key.
Chapter 3 – Running the Protected Application	Describes how the protected application uses network licenses, including information about obtaining, maintaining and releasing licenses.
Chapter 4 – Using the Monitoring Tool	Instructions for using the SentinelSuperPro Monitoring Tool to track and analyze license use across your network.
Chapter 5 – Updating Your Keys	Instructions for using the SentinelSuperPro Field Exchange Utility or Client Activator to update your keys.
Appendix A – Glossary	A glossary of SentinelSuperPro and software protection terms used throughout this manual.

Getting Help

For assistance with SentinelSuperPro or the protected applications that use it, please contact your software vendor first. If additional assistance is required, please contact Rainbow Technologies at <http://www.rainbow.com>.

Using Online Help

The SentinelSuperPro Monitoring Tool ships with a complete online Help system. It includes a table of contents and thorough index searching capabilities.

Help is very easy to use. To access online Help in the Monitoring Tool, select **Help** from the **Help** menu.

We Welcome Your Comments

To help us improve future versions of SentinelSuperPro documentation, we want to know about any corrections, clarifications or further information you would find useful. When you contact us, please include the following information:

- The title and version of the guide you are referring to
- The version of SentinelSuperPro you are using
- Your name, company name, job title, phone number and e-mail address

Send us e-mail at:

techpubs@rainbow.com

Or, you can write us at:

**Rainbow Technologies, Inc.
50 Technology Drive
Irvine, CA 92618**

Attn: Technical Publications Department

Thank you for your feedback.

Chapter 1

Getting Started

SentinelSuperPro 6.1 is a software toolkit that your software vendor used to create the protected application you have purchased. The application uses SentinelSuperPro to support the licensing agreement you have with your vendor by authorizing and metering application use. As a result, Sentinel-SuperPro software must be installed on your server and/or client computers in order for the protected application to work properly.

As a system administrator, you are responsible for installing the protected application, as well as the SentinelSuperPro software. You will also be responsible for monitoring application use and assisting your users with any problems they may have with accessing the application.

This chapter explains how a SentinelSuperPro-protected application works, introducing you to the concepts you need to understand before you install and use the SentinelSuperPro software with the protected application.

This chapter covers the following topics:

- How a SentinelSuperPro-protected application works
- The difference between stand-alone and network applications
- What's included with a SentinelSuperPro-protected application
- System requirements for using SentinelSuperPro software

How Does a SentinelSuperPro-Protected Application Work?

Your software vendor has selected the SentinelSuperPro system as a means of controlling access to and use of the application you have purchased. A SentinelSuperPro-protected application uses a *hardware key* to control how many users can run the application, as well as the features those users will have access to.

Stand-alone v. Network Applications

There are two types of SentinelSuperPro-protected applications: *stand-alone* and *network*.

- A *stand-alone* application is licensed to run on a single computer without using a network. This type is used most often when an application is used by a single person on a particular computer. The application and SentinelSuperPro software are installed on that computer, along with a hardware key. When the application starts, it communicates with the hardware key through the SentinelSuperPro server. Without the hardware key, the application cannot be used.

Typically, when you have purchased a stand-alone application, you will receive a hardware key for each user that will be running the application. Additionally, the SentinelSuperPro server software must be installed on each user's workstation to use a stand-alone application.

- A *network* application is designed to be run on multiple computers so that several users can share it. In this case, a network is required so that all computers that are authorized to use the application are connected. The SentinelSuperPro server must be installed on one or more computers on the network to coordinate the use of the application, but, unlike stand-alone applications, it does not have to be installed on each workstation the application will be run on.

How Does a SentinelSuperPro-Protected Application Work?

Only one hardware key is required for a network application; this key is connected to a server on the network. When the application starts, instead of communicating with a hardware key connected directly to the client computer, the application communicates instead with a server and key located elsewhere on the network. The SentinelSuperPro server acts as a link between the application on the client computer and the key located on the server.

Keys used with network applications contain multiple *licenses*, so that a user from across the network can access the key remotely, obtain a license, and then run the application from her local workstation. When the maximum number of licenses have been obtained, no other users can run the application until a license has been released by a user closing an already running application.

What Is a License?

When you purchased the protected application, you made an agreement with your software vendor that you would use only a certain number of instances of the application at any one time—these are your rights to the application. These rights are stored in digital form as *licenses*. Licenses determine both who can use the application, and where the application can be used.

The *license limit* indicates the maximum number of concurrent users of the application. Each instance of an application uses a license when it is started.

For example, if the software vendor gave you rights to have 10 users concurrently running the application, then you have 10 licenses. Each time a user starts the application, the license count is decremented by one. Thus, if two users are running the application, you have only eight licenses left. Once all 10 licenses are being used, no other instances of the application can be run anywhere on the network until one of the licenses currently in use is released. A license is released when a user closes the application.

Sublicensing

Depending on how the software vendor has set up his application protection, the protected application may also use *sublicensing* to control access to the application.

On each key, a *hard license limit* has been encoded. This limit is set at the factory when the key is manufactured, and cannot be changed through software. Thus, if a software vendor wants to enforce a license limit that is less than the hard limit, sublicensing is used.

For example, if all hardware keys are encoded with a hard limit of 10, but the software vendor wants to limit use of the application to 5 concurrent users, he sets the *sublicense limit* to 5.

While as a system administrator you do not have any control over the sublicense limit, it is important that you understand the concept of sublicensing. This is because when you view hardware keys using the SentinelSuperPro Monitoring Tool (see page 7), the hard limit is displayed. If the hard limit is greater than the sublicense limit being used, if any, it may *look* like more licenses are available than are actually usable. This is why a key may seem to have 10 licenses available, but only 5 users can run the application at any one time; in this case, a sublicense limit of 5 has been set by your software vendor.

If your vendor is using sublicensing, there is no way for you to view the actual number of licenses available on a key. Contact your software vendor more information about the number of licenses available to you.

A Note About Licenses

Throughout this manual, we refer to *obtaining* and *releasing* licenses. Although it is convenient to describe license management in this way, in actuality, licenses are never physically moved between the server/key and the client workstation. Instead, the SentinelSuperPro server simply keeps track of how many users can run the application and decrements and increments the license count as authorized users are granted permission to run the application and as they exit the application.

What Is the SentinelSuperPro Server?

The SentinelSuperPro server coordinates the use of the protected application by multiple users and computers over a network. When a client needs to access a SentinelSuperPro hardware key to obtain a license for the protected application, the server acts as a link between the client and the key.

The server maintains and processes license information for the protected application. The server communicates with the key through the Sentinel driver to obtain information about the license limit encoded on the key. Because the server maintains all licenses, it is aware of how many licenses are being used at any one time. Together with the license limit information from the key, the server is then able to determine whether or not a license is available.

Because the server is the means of communication between the key and the protected application, all workstations that have a key connected must have the server software installed, even if the application is a stand-alone application.

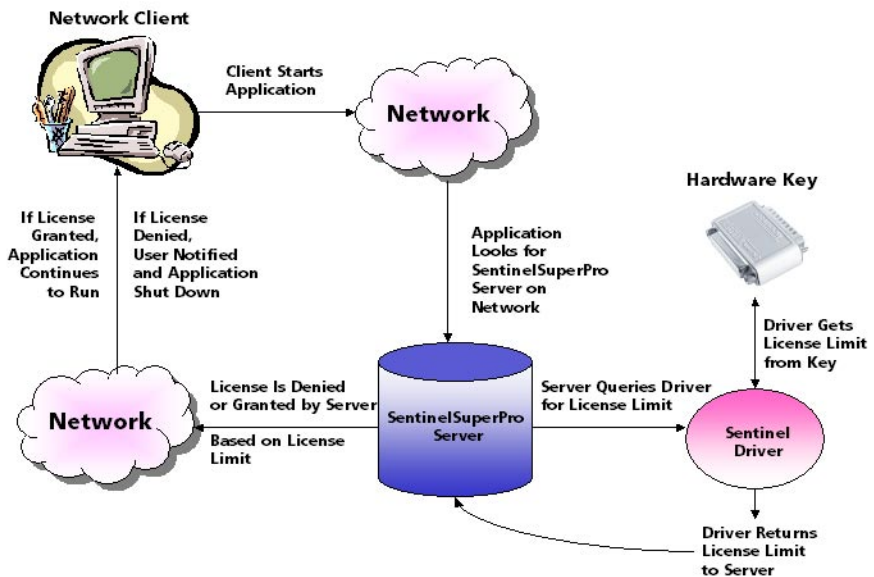
How an Application Obtains a Network License

When you start a protected application, the application must first communicate with a hardware key to verify that a license is available. When a stand-alone application is started, it checks for the presence of the key on that computer via the server installed on that computer.

But when a network application is started, it must obtain a license from a key located on the server. A license is obtained through the following steps:

1. The application sends a message over the network looking for a SentinelSuperPro server with a connected hardware key.
2. When a hardware key is found connected to an available server, the application requests a license.
3. The server queries the Sentinel driver to obtain the license limit from the hardware key.

4. The driver returns the license limit to the server.
5. If a license is available, the server grants the license. If all licenses are in use, the server denies the license request.
6. The server communicates the license status—granted or denied—to the client.
7. One of the following occurs:
 - If the license was granted, the application continues to run.
 - If the license was denied, the user is notified that no licenses are available, and the application is shut down.



How an Application Obtains a License over the Network

What Is the SentinelSuperPro Monitoring Tool?

The SentinelSuperPro Monitoring Tool allows you to view and keep track of the SentinelSuperPro servers on your network. With this tool, you can:

- See all the SentinelSuperPro servers currently installed and running on your network
- View the address and version of each available server
- View each of the keys connected to available servers
- View the hard license limit for each key
- Track how many licenses are currently in use
- View the highest number of licenses issued by a key
- Monitor the number of time-outs recorded by the server for clients using licenses from a key

The Monitoring Tool is a convenient way to view and track license activity on your network so that you can analyze application usage. For example, you could use the Monitoring Tool to determine whether or not you purchased enough licenses, based on license demand.

For more information about using the Monitoring Tool, refer to Chapter 4, “Using the Monitoring Tool,” on page 31.

What's Included with the Protected Application?

In addition to the items that make up the protected application's package, the following SentinelSuperPro items should also be included:

1. SentinelSuperPro 6.1 server software
2. SentinelSuperPro 6.1 Monitoring Tool software
3. Sentinel system driver
4. Field Exchange Utility (*FieldExUtil.exe*) or Sentinel Client Activator
5. Adobe Acrobat Reader (for accessing online documentation in PDF format)
6. One or more SentinelSuperPro hardware keys
7. This guide
8. Sentinel Client Activator documentation (only if your software vendor chose to use the Client Activator as a means of updating keys in the field; see Chapter 5, "Updating Your Keys," on page 37 for more information)

If you are missing any of these items, please contact your software vendor.

Note: Typically, all required SentinelSuperPro software should be included as part of the protected application's installation program. Contact your software vendor for more information on installing the SentinelSuperPro software.

SentinelSuperPro Software System Requirements

Review the following hardware and software system requirements prior to installing the SentinelSuperPro software.

Note: *Client system requirements for using the SentinelSuperPro-protected application can be found in the application's documentation.*

Minimum Hardware Requirements

- Pentium microprocessor, P90
- VGA monitor (800 x 600 resolution recommended)
- 35 MB free hard disk space
- CD-ROM drive
- 32 MB RAM

Minimum Software Requirements

- Microsoft Windows NT 4.0 Workstation with Service Pack 4 installed, Windows 95, Windows 98, Windows ME or Windows 2000
- One of the following network protocols: TCP/IP or Microsoft IPX/SPX
- Microsoft Internet Explorer 4.01 or higher (to view the SentinelSuperPro online Help file)

Go to <http://www.microsoft.com> on the Web to install a free version of Internet Explorer.

Note: *You **must** have Internet Explorer 4.01 or higher installed to be able to view the SentinelSuperPro Monitoring Tool online Help file. This file **cannot** be viewed with any other browser, such as Netscape Communicator.*

Chapter 2

Installation

To use a SentinelSuperPro-protected application, either on your network or as a stand-alone application, you must install and configure the SentinelSuperPro software. You also need to connect the SentinelSuperPro hardware keys to your client workstations or network servers.

The protected application's installation program should include all necessary SentinelSuperPro software; you should not need to run a separate setup program. However, your software vendor may have selected a different means of installing the SentinelSuperPro software; if you have any questions about installing the software, please contact your software vendor.

This chapter covers the following topics:

- Where to install the server
- Where to install the protected application
- SentinelSuperPro software installation information
- Configuring the server log files
- Setting the client environment variable
- Installing the hardware key

Where Should You Install the Server?

No matter which type of application you are using, stand-alone or network, the SentinelSuperPro server must be installed and configured for use with the application. Read the following sections to determine where you need to install the server for use with the protected application you have purchased.

Server Installation for Stand-alone Applications

If you will be running a stand-alone application, the server must be installed on the same workstation as the application itself. So, if you have five users who will be running the stand-alone application, you must install the SentinelSuperPro server on **each** of those users' workstations.

Each workstation the server is installed on must also meet the server system requirements, in addition to any system requirements for the protected application; see “SentinelSuperPro Software System Requirements” on page 9 for more information.

Server Installation for Network Applications

If you will be running a network application, the server can be installed on any computer that is located on the network and that meets the server system requirements (see “SentinelSuperPro Software System Requirements” on page 9).

Typically, the server should be located on the same subnet as the clients that will be running the protected application.

Installing Multiple Servers on the Network

If necessary, you can install multiple servers on the network, as long as you have a hardware key for each server. Because licenses are ultimately enforced according to the limit on the attached key, you can install as many servers as you have hardware keys.

For example, if you have clients on two separate subnets, both of which will be using the protected application, you should install two servers—one located on each subnet.

Where Should You Install the Protected Application?

The protected application must be installed on every workstation where a client will run the application, no matter whether it is a stand-alone application or a network application.

Because your license agreement with your software vendor is enforced through the SentinelSuperPro server and the attached hardware key(s), you can install the protected application on as many workstations as you like. However, the application will be able to be run simultaneously only on as many workstations as allowed by the server, based on the license limit contained in the hardware key(s).

If it is a stand-alone application, the application **must** be installed on the same system(s) where you installed the SentinelSuperPro server. If it is a network application, you may decide to not install the application on the same system as where you installed the server, if the application will not be run from that system.

For detailed instructions on installing the protected application, including system requirements, please refer to the documentation provided by your software vendor.

SentinelSuperPro Software Installation Notes

The following are some important notes about SentinelSuperPro software installation:

- The following SentinelSuperPro components are typically installed with SentinelSuperPro-protected applications:
 - SentinelSuperPro Server
 - SentinelSuperPro Monitoring Tool (required only for network applications)
 - Sentinel system driver
 - Sentinel Client Activator or Field Exchange Utility
- The Sentinel system driver is required to run all SentinelSuperPro software and SentinelSuperPro-protected applications. Do not uninstall this driver from any systems running the protected application.
- On Windows 95/98/ME, a registry entry is created that will start the server automatically whenever you boot up.
- On Windows NT/2000, the SentinelSuperPro server is installed as a system service that will start automatically whenever you boot up.
- If you will be running only stand-alone applications, the Monitoring Tool may not be necessary—it is up to you if you want to install this tool. However, if you will be running a network application, we strongly recommend installing this tool so you can keep track of where and when the protected application is being used. See Chapter 4, “Using the Monitoring Tool,” on page 31.
- The Field Exchange Utility or Sentinel Client Activator should be installed only on a system where a key will be connected (either a client workstation or a server). This is because keys cannot be updated over a network. See Chapter 5, “Updating Your Keys,” on page 37 for more information.

Configuring the SentinelSuperPro Server Log Files

If you want to be able to keep track of all transactions and errors processed by the SentinelSuperPro server, you need to 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.

If you are running Windows 95/98/ME, you will need to reboot your system once you have set the log file locations. You do not need to shut down the server first.

If you are running Windows NT/2000, prior to setting the log file locations, you must shut down the server if it is already running. Once the log file locations have been set, you can restart the server. You do not need to reboot your system.

For information about viewing the log files, see “Viewing the Transaction and Error Log Files” on page 36.

Shutting down the Server in Windows NT or 2000

1. Do one of the following:
 - In Windows NT, from the **Start** menu, point to **Settings > Control Panel**.
 - In Windows 2000, point to **Settings > Control Panel > Administrative Tools**.
2. Double-click on the **Services** icon.
3. In the dialog box that appears, select **SuperPro Server**.
4. Click **Stop**.
5. Once the service has been stopped, close the dialog box.

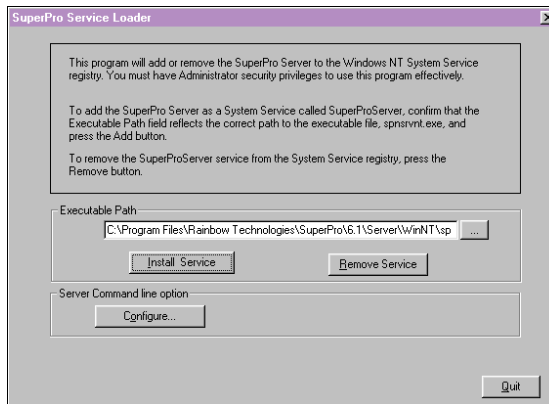
Setting the Log File Locations

To set the log file locations:

1. Locate the following file on your computer: *loadserv.exe*.

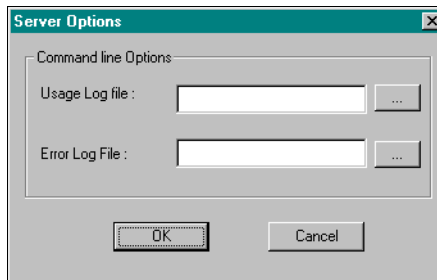
The location of this file may differ depending on how your software vendor configured the installation program.

2. Double-click on the *loadserv.exe* icon to run the file. The following screen appears:



SuperPro Service Loader

3. Click **Configure**. The following dialog box appears:



Server Options Dialog Box

4. Click the browse button to the right of the **Usage Log File** field to browse for the location where you want the log file to be written to.

You must enter a file name (such as *SSP error log.txt*) for the log file at the end of the path. If no file name is identified, a log file will not be created.

5. Repeat step 4 for the error log file.

Note: *You can set locations for only one log file, if desired. You do not need to set both locations in order to create only one log file.*

6. Click **OK**. You are returned to the Service Loader screen.
7. Click **Quit**.
8. Do one of the following:
 - If you are running Windows 95/98/ME, reboot your system so that logging will take effect.
 - If you are running Windows NT/2000, restart the server as explained in the following section.

Note: *You can also set the log file locations by adding an entry to the Windows Registry. Add the following entry to \\HKEY_LOCAL_MACHINE\\SOFTWARE\\RAINBOW TECHNOLOGIES\\SUPERPRO: NSOPTS="-l nsplog -ferrlog". Using this method, the log files will be created in the same directory where the server executable file is located.*

Starting the Server

To start the server in Windows NT/2000:

1. Do one of the following:
 - In Windows NT, from the **Start** menu, point to **Settings > Control Panel**.
 - In Windows 2000, point to **Settings > Control Panel > Administrative Tools**.
2. Double-click on the **Services** icon.
3. In the dialog box that appears, select **SuperPro Server**.
4. Click **Start**.
5. Once the service has started, close the dialog box.

Setting the Client Environment Variable

After you have installed the protected application and the SentinelSuperPro software, you need to configure an environment variable on each of your client workstations. The client environment variable NSP_HOST tells the protected application which server to look for when it needs to access a SentinelSuperPro key. The possible values for this variable are as follows:

- **no-net:** Tells the application to act as a stand-alone application. The application will look for a key *only* on the client machine. If the key is not found, the application will *not* send a broadcast message to the network looking for a server and key. Note that this value is case-sensitive.
- **server host name, IP address or IPX address:** Tells the application to act as a network application. The application will look for a key *only* on the selected server.

If the selected server is not found, or a key is not found on the selected server, the application will *not* send a broadcast message to the network looking for another server and key.

Setting this variable is optional; however, for maximum performance, we recommend this variable be set on each client workstation. If you do not set this variable, each time the application needs to access a SentinelSuperPro key, it will look first on the local machine, and then send a broadcast message to the network, searching for an available server and key on the network.

Sending broadcast messages not only requires use of network resources, it also takes longer, meaning the application will take longer to load and be ready for use. Setting this variable can save you both time and network resources, because the application will contact *only* the server you have defined in the NSP_HOST variable.

Note: *Your software vendor also can control through code how the protected application will search for a key. So, even if you set the NSP_HOST variable, it is possible the variable will be ignored because the vendor directed the application through code to act as a stand-alone or network application. Contact your software vendor for more information.*

To set the NSP_HOST variable:

1. From the **Start** menu, select **Settings > Control Panel**.
2. Double-click the **System** icon. The System Properties dialog box appears.
3. Click the **Environment** tab. Lists of existing system and user variables appear.
4. In the **Variable** field, enter **NSP_HOST**.
5. In the **Value** field, enter *one* of the following:

- **no-net**
- the SentinelSuperPro server's **host name**
- the SentinelSuperPro server's **IP address**
- the SentinelSuperPro server's **IPX address**

Refer to page 19 for a description of these possible values.

6. Click **Set**.

The NSP_HOST variable is added to the User Variables list, and is now available on a system-wide basis.

7. Click **OK** to close the System Properties dialog box.

Note: *Environment variables may also be set through a DOS command prompt window. However, when using this method, the variable will need to be reset each time the protected application is run, and the application must be run through the DOS window instead of through Start > Programs or Windows Explorer. For these reasons, we recommend setting a system-wide variable through the Control Panel, as explained above.*

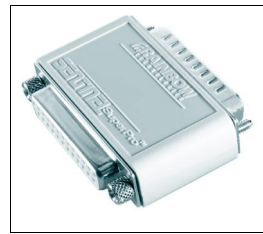
Installing the SentinelSuperPro Hardware Key

Included with the protected application are SentinelSuperPro hardware keys. These hardware keys allow you to access and run the application.

Depending on how your software vendor has configured the application, you may need only one key connected to a server on your network (for network applications), or you may need several keys, one for each workstation the application will be run on (for stand-alone applications).

In either case, the key **must** be connected to your server or workstation while you run the protected application. Network keys (used with network applications) can be identified by the phrase “SuperProNet” stamped into the plastic on one side of the key.

SentinelSuperPro hardware keys come in two form-factors: *parallel port* or *USB*. The type you received in your package depends on what you specified when you placed your order.



SentinelSuperPro USB Key (left) and Parallel Port Key (right)

Parallel port keys (25-pin or 36-pin) connect to a parallel port located on the back of your computer. USB keys connect to a USB port located on the back or front of your computer or on a USB hub. Use the instructions in the appropriate following section to install your hardware key.

Note: *USB hardware keys can be used with Windows 98/ME or Windows 2000 workstations only.*

Installing the Parallel Port Hardware Key

The SentinelSuperPro key can be attached to any parallel port on the server or workstation.

1. Locate an available parallel port on the computer you are installing the key on.

If your computer has only one parallel port, you may need to temporarily remove any existing parallel port devices (such as a Zip drive or printer) in order to connect the key. These devices may be reconnected to the key's outside connector after you have installed the key.

2. Attach the key to the parallel port connector.

Tip: *If your computer is close to a wall or other obstacle, you can attach an extension cable to the port, then attach the key to the cable. Use a straight-through DB-25 male-to-DB-25 female cable.*

3. Tighten the screws to connect the key securely to the port.
4. If necessary, reconnect any other parallel port devices to the outside connector on the key.

We recommend using a shielded printer cable if you are connecting a printer to your computer through the SentinelSuperPro key.

Connecting Multiple Parallel Port Keys

Up to 10 SentinelSuperPro keys—parallel port or USB keys in any combination—can be connected to the same computer.

If you are using parallel port keys, multiple SentinelSuperPro keys can be attached to the same parallel port; this is called *cascading*.

The number of keys that can be cascaded is dependent on the system they are attached to. Refer to your system's documentation for more information about attaching devices to your parallel port.

SentinelSuperPro keys can also be cascaded with other Rainbow Technologies keys that support cascading. Make sure the SentinelSuperPro keys are the *last* keys in the chain (farthest from the computer).

Warning! *There is one exception to this rule. If you are cascading SentinelSuperPro keys with Rainbow Technologies' NetSentinel keys, the SentinelSuperPro keys **must be located before any NetSentinel keys** in the chain. NetSentinel keys should be the last keys in the chain. If SentinelSuperPro keys are located behind NetSentinel keys, they will not be recognized by the Sentinel driver, and thus the protected application will not run.*

While SentinelSuperPro keys can be cascaded with keys from other companies, this may cause compatibility issues and is not recommended.

Keys can also be connected to up to four parallel ports on the same computer. For example, if you have four parallel ports on your computer, you could attach a separate key to each port simultaneously. The Sentinel driver automatically polls all parallel (and USB) ports when looking for a key.

Installing the USB Hardware Key

If you have multiple USB ports (if, for example, you are using a USB hub), you can connect multiple USB hardware keys to a single computer, as long as you don't exceed a total of 10 SentinelSuperPro keys—parallel port or USB keys in any combination.

Cascading—connecting multiple keys to the same port—is not supported for SentinelSuperPro USB hardware keys.

1. Locate an available USB port on your computer.
2. Attach the key to the USB port. Make sure it is securely and tightly connected.

Note: *Remember, USB hardware keys can be used with Windows 98/ME or Windows 2000 workstations only.*

Installing Keys after the Server Is Already Running

If you already have a SentinelSuperPro server running on your network, additional keys can be installed at any time without having to reboot the server—this is called *hotplugging*.

The SentinelSuperPro server automatically detects any new keys that have been attached since the last time the server was started. This allows you to connect a new key to the server without shutting down the server and terminating those clients currently accessing the key and running the protected application.

To add a new key to a server, do one of the following:

- Connect a USB key to an available USB port on the server or hub connected to the server.
- Connect a parallel port key to an available parallel port on the server, or, cascade the key with an existing SentinelSuperPro key by connecting the new key to the existing key. See page 22 for more information about cascading.

Remember, you can have a maximum of 10 keys—parallel port or USB—connected to a single computer.

Where to Go Next

Once you have installed the protected application and SentinelSuperPro software, configured the client environment variable, set the log file locations and installed the SentinelSuperPro hardware keys, you are ready to run the protected application.

Go to Chapter 3, “Running the Protected Application,” on page 27.

Chapter 3

Running the Protected Application

All SentinelSuperPro-protected applications must obtain a license before they can be run. Licenses determine both who can use the application and where the application can be used. Each instance of an application uses a license when it is started.

When a protected application is run, it will locate a key, obtain a license, maintain the license by sending messages back to the server, and then release the license when it is no longer needed.

This chapter explains how both stand-alone and network applications obtain and use licenses.

This chapter covers the following topics:

- How a key is located
- How a license is obtained
- How a license is maintained
- When a license is released

How the Application Locates a Key

Before your application can obtain a license, it must first locate a SentinelSuperPro hardware key either on the local machine or somewhere on the network. Where and how the application locates a key is dependent on whether the application is a stand-alone application or a network application.

How a Stand-alone Application Locates a Key

When a protected application is in stand-alone mode, it looks for a key on the local machine. If a key is not present locally, the application will not go to the network to find a key. It will simply return an error message that a key cannot be found.

If the key is found, the application starts normally and communicates with the key through the server (which must also be installed on the same workstation) to obtain a license.

How a Network Application Locates a Key

When your application is in network mode, it will go immediately to the network to locate a key, ignoring the local USB and parallel ports completely.

If a specific server to contact was set in code or through the `NSP_HOST` variable (see page 19), the application will look only for the specified server. If the server cannot be located, an error message appears and/or the application shuts down.

If a specific server to contact was not identified in code or the `NSP_HOST` variable, the application sends a broadcast message to the network to find out which servers are available.

The broadcast message is sent to the subnet the application is running on. Once the first server responds, the application attempts to obtain a license from that server. If the contacted server has a license available, the application obtains the license from that server. If that server does not have any licenses available, the application will then contact other servers that responded to the broadcast message to try to obtain a license.

How the Application Obtains a License

All license information is maintained by SentinelSuperPro server software installed on the client machines or the servers on the network.

Before an application can be started, it must first obtain a license from the SentinelSuperPro server. The server issues a license only if the *license limit* in the key has not yet been exceeded. The license limit indicates the maximum number of concurrent users of the application. Once a key is located, the way in which a license is obtained is the same for both stand-alone and network applications.

Note: *Remember, whether the application is stand-alone or network, it always uses the SentinelSuperPro server as the means of communicating with the key. This is why the SentinelSuperPro server must be installed on the same system as stand-alone applications, and on a server located on the network for network applications.*

The process for obtaining a license is as follows:

1. Once a hardware key is found, the application requests a license.
2. The SentinelSuperPro server queries the Sentinel driver to obtain the license limit from the hardware key.
3. The driver returns the license limit to the SentinelSuperPro server.
4. If a license is available, the SentinelSuperPro server grants the license. If all licenses are in use, the server denies the license request.
5. The SentinelSuperPro server communicates the license status—granted or denied—to the client.
6. One of the following occurs:
 - If the license was granted, the application continues to run.
 - If the license was denied, the user is notified that no licenses are available. An error displays or the application is shut down.

How the Application Maintains the License

Once a license has been obtained, the application must maintain the license by sending “heartbeat” messages to the server, confirming the client is still using the license.

These periodic messages are sent automatically every 60 seconds. If the server does not receive a heartbeat message from the client, it will release the license and send an error to the application. An error is also returned if the application sends a heartbeat message after the license has already been released.

When the Application Will Release the License

There are three situations in which a license will be released:

- The client has shut down the protected application
- The client fails to send a heartbeat message to the server
- The application has completed all key operations

Chapter 4

Using the Monitoring Tool

The SentinelSuperPro Monitoring Tool allows you to view and keep track of the SentinelSuperPro servers on your network. The Monitoring Tool is a convenient way to view and track license activity on your network so that you can analyze application usage. For example, you could use the Monitoring Tool to determine whether or not you purchased enough licenses, based on license demand.

This chapter assumes you are running a network application, and have a SentinelSuperPro server installed on only one workstation on the network. Typically, the Monitoring Tool is not used with stand-alone applications.

This chapter covers the following topics:

- Starting the Monitoring Tool
- Viewing servers and keys on the network
- Searching for specific servers
- Viewing the server transaction and error log files

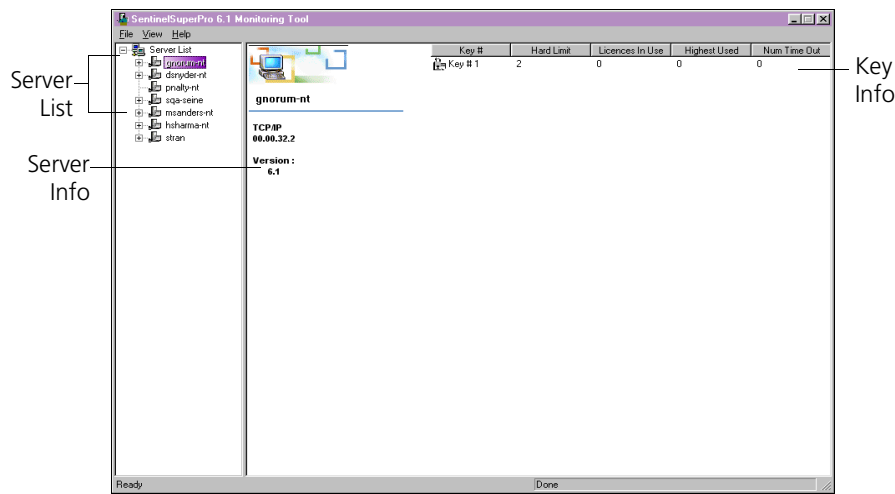
Starting the Monitoring Tool

The Monitoring Tool should have been installed on the same workstation the SentinelSuperPro server was installed on.

To start the Monitoring Tool:

- From the **Start** menu, select **Programs > Rainbow Technologies > SentinelSuperPro 6.1 > Monitoring Tool**.

The following screen appears:



SentinelSuperPro Monitoring Tool

Viewing Servers and Keys

When you start the Monitoring Tool, it automatically scans the network for all running SentinelSuperPro servers. This may take a few minutes. Once the servers have been located, they appear in the server list located in the left pane of the Monitoring Tool window.

Viewing Server Information

To view additional information about a server, click on a server in the list to view the following information in the right pane:

- The server name
- The server's protocol (TCP/IP or IPX/SPX)
- The server's address (for both protocols, if applicable)
- The server's version
- Key information for each key connected to the server

Viewing Key Information

When you expand a server in the tree, under each server, a list of the keys attached to that server appears. To view additional information about an individual key, click on the key name. The following information appears in the columns located in the right pane:

- **Key #:** The key's number (a label used only for identification purposes).
- **Hard Limit:** The maximum number of licenses that are available on this key.

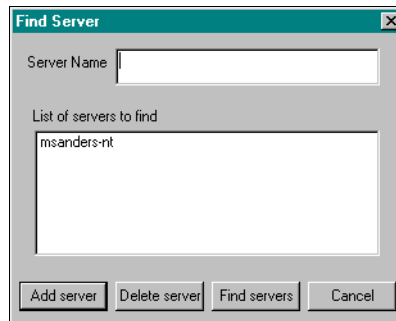
If your software vendor implemented sublicensing, the actual number of maximum available licenses may be lower than the hard limit. See "Sublicensing" on page 4 for more information.

- **Licenses in Use:** The number of licenses currently being used by clients on the network running the protected application.
- **Highest Used:** The highest number of licenses used by clients during this session.
- **Num Time Out:** The number of clients who obtained a license, but were timed out by the server. Time-outs can occur if the client fails to contact the server and key on a regular basis to maintain the license.

Searching for a Specific Server

If a server on the network does not appear in the server list, you can search for it. To search for a server:

1. From the **View** menu, select **Find**. The Find Server dialog box appears.



Find Server Dialog Box

2. In the **Server Name** field, enter the host name or address of the server you are looking for.
3. Click **Add Server** to add the server to the list of servers to search for.
4. Click **Find Server** to search for the server (and any other servers in the list). If the server is found, it appears in the server list in the left pane.

Once a server has been added to the list of servers to search for, it will remain on the list until you remove it. To remove a server from the list, select the server and then click **Delete Server**.

Refreshing the Server List

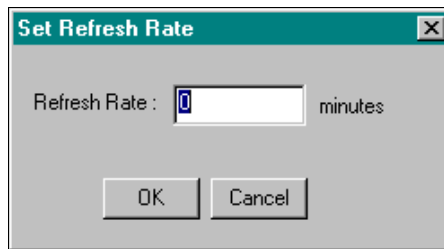
To view any newly-started servers on the network, or remove servers that were shut down since the last refresh, you can manually refresh the server list.

- To refresh the server list, from the **View** menu, select **Refresh**.

The Monitoring Tool can also automatically refresh the server list, looking on the network for newly-started servers and removing servers that have been shut-down, at an interval that you set. The refresh rate is measured in minutes.

To set the refresh rate:

1. From the **View** menu, select **Set Refresh Rate**. The Set Refresh Rate dialog box appears.



Set Refresh Rate Dialog Box

2. Enter the new refresh rate in minutes.
3. Click **OK**.

Viewing the Transaction and Error Log Files

If you set log file locations before you started the SentinelSuperPro server, the server records all transactions and errors that occur during a session in two log files: the transaction log file and the error log file.

The error log file records information about server startup and status. Any errors that occur are recorded in this log file.

The transaction log file records information about the clients that connect to the server and the licenses being used by those clients. The following information is contained in the transaction log file:

- The operation that took place:
 - 1 = issue license
 - 2 = release license
 - 3 = timeout
 - 4 = key access
 - 5 = startup
 - 6 = shutdown
- Date/time information
- Host name
- Client name
- Client process ID
- Operation return code
- License key
- Licenses in use
- Sublicense key information
- Key index

Note: *Only information about network clients is recorded in the log files. Information about clients using stand-alone applications is not included in the log files.*

To view the log files, locate the files in the paths you defined when you set the log file location. See “Setting the Log File Locations” on page 16 for more information.

Chapter 5

Updating Your Keys

SentinelSuperPro's **Secure, Authenticated Field Exchange** (SAFE, also known as *field activation*) protection system allows your software vendor to remotely update your SentinelSuperPro hardware key's memory.

Field activation allows your vendor to increase demo limits, upgrade demo applications to fully licensed versions, and provide access to additional modules or features, without having to ship you a new key or visit your site.

As a customer, you are responsible for generating a locking code that you send to your software vendor. The vendor then uses the locking code to generate a license code that is returned to you. The license code updates the key and activates the protected application appropriately.

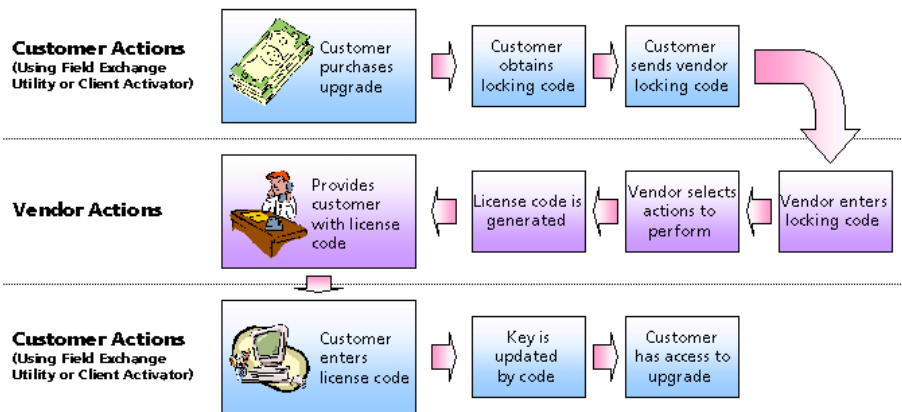
This chapter covers the following topics:

- How are keys updated?
- Using the Sentinel Client Activator
- Using the Field Exchange Utility

How Are Keys Updated?

SentinelSuperPro keys are updated remotely as a result of information exchanged between you and your software vendor. All exchanged information is encrypted and secure, and cannot be used to update any other SentinelSuperPro key.

The key update process is as follows:



Customer and Software Vendor Roles in Key Activating or Updating

1. You purchase additional services, such as a higher license limit, or added features.
2. You use the Sentinel Client Activator or the SentinelSuperPro Field Exchange Utility to generate a *locking code*.
3. You send the locking code to your software vendor via telephone, fax, e-mail or the Internet.
4. The software vendor generates a *license code*—specific to your key—based on the locking code you generated.
5. The software vendor sends the license code back to you.

6. You enter the license code in the Client Activator or Field Exchange Utility.

The license code tells the Field Exchange Utility or Client Activator how to reprogram the key.

7. The key is updated and you have access to the services you purchased.

What Is a Locking Code?

The locking code for a key includes information about how the key is currently programmed. Your software vendor must have a customer-generated locking code to create a license code.

Locking codes are unique for each key.

What Is a License Code?

The license code for a key describes the actions to be performed on a key in the field. It determines how the application will be updated; for example, what new features you will have access to, or the number of additional licenses that will be added.

The license code is generated by SentinelSuperPro based on the locking code you send to the software vendor. When you enter the license code in the Client Activator or Field Exchange Utility, a script is automatically run that updates the key.

License codes are unique to the key the locking code was generated from.

Using Client Activator

The Client Activator is Rainbow Technologies' recommended means of field activation for SentinelSuperPro protected applications, due to its user-friendly interface. The Client Activator allows you to easily and quickly activate your product via a Web site, if your software vendor has selected the Web update option.

Client Activator System Requirements

You must be running one of the following operating systems in order to use the Client Activator:

- Windows 98
- Windows ME
- Windows NT 4.0
- Windows 2000

Additionally, if your software vendor allows product activations and upgrades over the Internet, you must use one of the following Internet browsers:

- Internet Explorer 4.01 or 5.0
- Netscape Navigator 4.6 or 4.7

Installing Client Activator

If your software vendor has decided to use Client Activator to update your keys remotely, the Client Activator installation program should have been included in the protected application's setup program, or on the application's CD-ROM.

In order to update keys, the Client Activator must be installed on the same system where the SentinelSuperPro key has been connected.

- If the protected application is a stand-alone application, the Client Activator should be installed on each client system.

- If the protected application is a network application, the Client Activator should be installed only on the server where the SentinelSuperPro key is located; it does not need to be installed on the client systems.

Please contact your software vendor for more information about installing and using Client Activator with the protected application.

If You Aren't Using the Client Activator

If your software vendor decided to not use the Client Activator for field activation and upgrades, you will need to use the SentinelSuperPro Field Exchange Utility to generate locking codes. Go to the next section for more information.

Using the Field Exchange Utility

The Field Exchange Utility is an alternative to the Client Activator. It is used to generate the locking code needed by your software vendor to generate a license code. You also use the Field Exchange Utility to enter the license code that updates your key.

Depending on how your software vendor has set up their application, you may or may not need to use this utility. Contact your vendor for more information about which key update utility to use.

Installing the Field Exchange Utility

If it will be used for key updating, the Field Exchange utility (*FieldExUtil.exe*) should have been installed automatically during application setup. No further installation is necessary.

In order to update keys, the Field Exchange Utility must be installed on the same system where the SentinelSuperPro key has been connected.

- If the protected application is a stand-alone application, the Field Exchange Utility should be installed on each client system.
- If the protected application is a network application, the Field Exchange Utility should be installed only on the server where the SentinelSuperPro key is located; it does not need to be installed on the client systems.

Contact your software vendor for more information about installing the Field Exchange Utility.

Verifying the SentinelSuperPro Server Is Running

To use the Field Exchange Utility, the SentinelSuperPro Server must be installed and running on the same workstation the utility is being used on. If the server is not running, you will be unable to generate locking codes.

Before opening the Field Exchange Utility, you should verify that the SentinelSuperPro server is installed and running. To verify the server is running:

- In Windows 98/ME, from the **Start** menu, point to **Programs > Accessories > System Tools > System Information**.

In the dialog box that appears, click on **Software Environment**. Then, under **Running Tasks**, look for *spnsrv9x.exe*. If this file is listed, the server is running.

- In Windows NT, from the **Start** menu, point to **Settings > Control Panel**, then double-click on the **Services** icon.

In the dialog box that appears, the SuperPro Server should be listed with a status of **Started**.

- In Windows 2000, from the **Start** menu, point to **Settings > Control Panel > Administrative Tools**, then double-click on the **Services** icon.

In the dialog box that appears, the SuperPro Server should be listed with a status of **Started**.

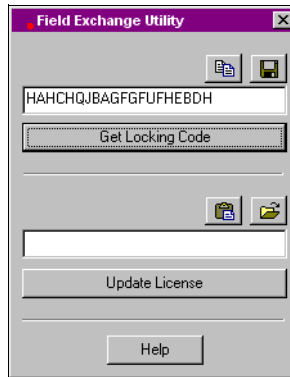
If the server is installed, but not running, do one of the following:

- In Windows 95/98/ME, locate and then double-click the *spnsrv9x.exe* file. The server will start automatically.
- In Windows NT, from the **Start** menu, point to **Settings > Control Panel**, then double-click on the **Services** icon. In the dialog box that appears, select **SuperPro Server**, then click **Start**.
- In Windows 2000, from the **Start** menu, point to **Settings > Control Panel > Administrative Tools**, then double-click on the **Services** icon. In the dialog box that appears, select **SuperPro Server**, then click **Start**.

Opening the Field Exchange Utility

To open the Field Exchange utility:

1. Verify the SentinelSuperPro Server is installed and running. See “Verifying the SentinelSuperPro Server Is Running” on page 43 for instructions.
2. Locate and then double-click the **FieldExUtil.exe** file icon.



Field Exchange Utility Window

Generating a Locking Code

To update the hardware key used to run your application, you must provide information about the key to your software vendor. The Field Exchange Utility displays this information in the form of a locking code, similar to the following:

EHBFGYARDIJABRFLEBDH

You must communicate the locking code to the software vendor as they have instructed (for example, via fax or e-mail). The vendor will then give you a corresponding license code to enter into the Field Exchange Utility.



To generate a locking code for a key:

1. Verify the correct hardware key is attached to the appropriate port on your computer.

2. Click **Get Locking Code**. The locking code appears in the top field.

If the message “Error” appears in the top field, make sure the key is firmly attached to the port and try again.

3. Do one of the following:

- Click the copy button  to place the locking code on the clipboard.
- Click the save button  to save the locking code to a file. Define a location and file name for the file, then click **Save**.
- Write down the code exactly as it appears in the field.

4. Send the locking code to the software vendor as directed.
5. Wait to continue the update process until you have received the license code from your software vendor. You can leave the Field Exchange Utility open, or you may close it. Either way, the license code you receive from your software vendor will update your key correctly.

Entering a License Code

The license code provided to you by the software vendor will reprogram the hardware key used to run the application, giving you access to the additional services or features you have purchased. License codes look the same as locking codes.

License codes are unique to the key they were generated for. License codes used with one key cannot be used to activate upgrades for another key, even if the application the key is used with is the same.

Thus, if you have several clients, each with their own key, you need to repeat the process of generating a unique locking code and entering a corresponding license code for *each* client’s key.



To enter a license code:

1. If necessary, open the Field Exchange Utility.

2. Verify the correct key is attached to your computer. Only one hardware key should be attached to your computer during the update process.

Note: *If you are updating a key located on a server, you **must** remove all other keys, leaving only the one you are updating. Only one key should be attached to the server during the update process. Because removing keys may terminate the application on some client systems, you may want to perform key updates only during non-peak hours.*

3. In the field above the **Update License** button, enter the license code given to you by your software vendor. Do one of the following:

- Click the paste button  to paste the code from the clipboard, if it was placed there.
- Click the open button  to load the code from a file. Browse to locate the file (.LIC), then click Open.
- Type the code in the field. Be sure to enter it exactly as it was provided.

4. Click **Update License**.

The key update process begins; it may take up to two or three minutes to complete the process.

5. When “Update Successful” appears, close the Field Exchange Utility.

The application is now ready to use, and you should have access to the additional licenses or new features you purchased.

Note: *If the update process is not successful, verify the key is securely attached to your computer and try again. If the process is still unsuccessful, or you do not have access to the upgrades you purchased when the process is complete, contact your software vendor for assistance.*

Appendix A

Glossary

D

demo	A demonstration or trial version of an application that uses a counter to control the number of times the application can run before it expires.
driver	A piece of software that enables the computer to communicate with a peripheral device (the SentinelSuperPro hardware key).

H

hard limit	Defines the maximum number of licenses that can be obtained from a key, and thus the maximum number of users (both local and across the network) that can access the protected application. The hard limit is programmed into each key at the factory and cannot be changed. <i>See also</i> hardware key , license , sublicense .
hardware key	The key controls and verifies access to the protected applications, assuring that only authorized users can run them.

L

license

A license allows you to start the protected application and access the hardware key. Licenses are never physically moved between the server/key and the client workstation. Instead, the SentinelSuperPro server simply keeps track of how many users can run the application and decrements and increments the license count as authorized users are granted permission to run the application and as they exit the application. *See also* **hard limit**, **sublicense**.

license code

A code that describes the actions to be performed on a key in the field. It determines how the application will be activated or updated.

The license code is generated by your software vendor based on the locking code you provide. When you enter the license code in the Client Activator or Field Exchange Utility, a script is automatically run that updates the key.

License codes are unique to the key the locking code was generated from.

locking code

A code that includes information about how a key is currently programmed. Your software vendor must receive a locking code from you in order to create a license code. Locking codes are unique for each key.

M

Monitoring Tool

A Windows application designed for use with protected applications intended to be run on a network. The Monitoring Tool displays information about all SentinelSuperPro servers, keys and user licenses in the field. The tool reports statistics, such as the number of licenses currently in use and the license limit for each key.

N

network key

Allows multiple network clients to access a protected application using a single hardware key. Network keys, which are typically connected to servers on the network, are programmed at the factory with a hard limit. *See also* **hard limit**, **hardware key**, **license**.

network mode

An access mode used for applications where *only* a network key can be used. The application will look for a key *only* on the server located on the network, ignoring the USB and parallel ports on the local machine.

S

server	The SentinelSuperPro server manages licensing and security for the protected application. The server is the link between the client running the application and the hardware key, located on the network, that responds to the API functions used in the application.
stand-alone mode	An access mode used for applications where <i>only</i> a local key can be used. The application will look for a key <i>only</i> on the client machine. If the key is not found, the application will <i>not</i> send a broadcast message to the network looking for a server and key.
stand-alone key	A key typically connected directly to a user's local workstation, providing access to the protected application only on a single system. These keys can also be connected to servers, but provide only a single license at any one time. <i>See also</i> network key, hard limit, license.
sublicense	A sublicense is a license limit your software vendor defined that is less than or equal to the hard limit programmed into the key. Sublicenses allow the vendor to implement fewer licenses for an application than the hard limit programmed on the key, protect several applications using the same key by defining separate license limits for each, and control concurrent access to specific features or modules within the protected application(s). <i>See also</i> hard limit, license.

U

USB

Universal Serial Bus. A technology that features one “universal” plug type for all USB peripheral-to-PC connections. USB replaces all the different kinds of serial and parallel port connectors with one standardized plug and port.

USB simplifies the connection of peripherals to computers by providing an instant, no-hassle way to connect USB peripherals. With USB-equipped PCs and peripherals are automatically configured and ready for use.

Appendix A – Glossary

Index

A

- accessing Help ix
- applications
 - locating key 28
 - network 2, 12, 28
 - protected 2, 13
 - stand-alone 2, 5, 12, 28

B

- broadcast messages 19, 28

C

- cascading keys 22, 23
- Client Activator
 - installing 40
 - requirements 40
 - use of 38
- client, configuring 19
- components,
 - SentinelSuperPro 8, 14
- configuring
 - client 19
 - server log files 15
- connecting keys 22–23
- contact server 28

D

- demo applications 47
- driver, system 14, 47

E

- entering license code 45
- environment variable,
 - configuring 19
- error log file 36
- errors, licensing 30
- extension cable 22

F

- field activation 37
- Field Exchange Utility
 - description 42
 - entering license code 45
 - generating locking code 44
 - installing 14, 42
 - opening 44
 - updating key with 46
 - use of 38
- files, log 15, 17, 36
- finding servers 34
- form-factors, keys 21

G

- generating locking code 44

H

- hard limit 4, 33, 47
- hardware keys
 - activating 38
 - cascading 22, 23
 - connecting 22–23
 - definition 47
 - description 2
 - form-factors 21
 - installing 21, 22–23
 - on server 24
 - license codes 39, 45
 - locating 28
 - locking codes 39, 44, 45
 - multiple 12
 - NetSentinel 23
 - network 3
 - parallel port 21–22
 - updating 38, 46
 - USB 21, 23
 - viewing information about 33
- hardware requirements 9

Index

heartbeat messages 30

Help, accessing ix

host name 19

hotplugging 24

I

installing

Client Activator 14, 40

Field Exchange Utility 14,
42

hardware keys 21–22

Monitoring Tool 14

multiple servers 12

protected application 13

Sentinel Client Activator
14, 40

SentinelSuperPro server 12,
14

SentinelSuperPro software
8, 11

Internet Explorer 9

IP address 19

IPX address 19

K

Key # 33

keys

See hardware keys

L

license code

definition 48

description 39

entering 45

license limit 3, 29

licenses

available 4

definition 48

description 3, 27

errors 30

in use 34

maintaining 30

obtaining 5, 29

releasing 30

with network applications 3

loadserv.exe 16

locating key 28

locations, log file 15

locking code

copying 45

definition 48

description 39

generating 44

saving to file 45

log files

name of 17

setting locations for 15

setting through registry 17

viewing 36

M

maintaining licenses 30

messages

broadcast 19, 28

heartbeat 30

Monitoring Tool

definition 49

description 7, 31

installing 14

starting 32

viewing

key information 33

server information 33

multiple

hardware keys

parallel port 22

USB 23

servers 12

N

NetSentinel keys 23

network application

installing Client Activator
for 41

installing Field Exchange
Utility for 42

locating key for 28

obtaining license for 5

network applications

description 2

installing server for 12

network keys 21, 49

network mode 49

no-net 19

NSP_HOST variable

setting 19

use of 28

O

obtaining licenses 5, 29

online Help, accessing ix

opening

Field Exchange Utility 44

Monitoring Tool 32

P

parallel port

devices 22

hardware keys 21–22

protected applications

how it works 2

installing 13

types 2

R

- refresh rate, setting 35
- refreshing server list 35
- releasing licenses 30
- requirements
 - Client Activator 40
 - system 9

S

- SAFE 37
- saving license code to file 45
- searching for servers 34
- Sentinel Client Activator
 - description 40
 - installing 14, 40
 - system requirements 40
- SentinelSuperPro
 - components 8, 14
 - description 1
 - software installation 8, 11
 - system driver 14
 - system requirements 9
- server list, refreshing 35
- server, SentinelSuperPro
 - definition 50
 - description 2, 5
 - finding 34
 - host name 19
 - install location 12
 - installation 14
 - installing for network applications 12
 - installing keys on 24
 - installing multiple 12
 - license maintenance 4
 - log files 15, 17, 36
 - shutting down 15
 - stand-alone installation 12
 - starting 18

- tracking 7
- updating keys on 46
- verifying running of 43
- viewing information about 33
- setting
 - log file locations 15, 17
 - NSP_HOST variable 19
 - refresh rate 35
- shutting down server 15
- software requirements 9
- stand-alone applications
 - description 2
 - installing Client Activator for 40
 - installing Field Exchange Utility for 42
 - installing server for 12
 - locating key for 28
 - obtaining license for 5
- stand-alone key 50
- stand-alone mode 50
- starting
 - Field Exchange Utility 44
 - Monitoring Tool 32
 - server 18
- sublicense limit 4
- sublicensing 4, 50
- SuperPro Service Loader 16
- system driver 14, 47
- system requirements 9, 21, 40

T

- time-outs 30, 34
- transaction log file 36

U

- updating hardware keys 38, 46
- USB
 - definition 51
 - keys 21, 23
 - ports 23
- USB keys 21

V

- variable, NSP_HOST
 - setting 19
 - use of 28
- verifying server is running 43
- viewing
 - key information 33
 - log files 36
 - server information 33

W

- Windows Registry log file
 - locations 17

