

*Quick Start
Guide*

SENTINEL SuperPro

 **RAINBOW**
TECHNOLOGIES

© 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.

CONFIDENTIAL INFORMATION

The SentinelSuperPro software protection system is designed to protect your software products from unauthorized use. The less information that unauthorized people have regarding your security system, the greater your protection. It is in your best interest to protect the information herein from access by unauthorized individuals. Please read the Developer's Agreement at the beginning of this guide for safeguarding requirements.

Part Number 700664-001, Revision B
Software releases 6.1 and later

Revision	Action/Change	Date
A	Initial Release	October 2000
B	Changed documentation 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 are located worldwide.



Software License and Developer's Agreement

All Products (including developer's kits, Sentinel hardware keys, diskettes or other magnetic media, software, documentation and all future orders) are subject to the terms stated below. If you disagree with these terms, please return the Product and the documentation to Rainbow, postage prepaid, within three days of your receipt, and Rainbow will provide you with a refund, less freight and normal handling charges.

1. You may not copy or reproduce all or any part of the Product, except as authorized in item 2 below. Removal, emulation or reverse-engineering of all or any part of the Product constitutes an unauthorized modification to the Product and is specifically prohibited. Nothing in this license permits you to derive the source code of the software files that Rainbow has provided to you. Your software programs must be protected or licensed using a licensed and registered copy of this Rainbow Product. Rainbow provides no other warranty to any person, other than the Limited Warranty provided to the original purchaser of this Product.
2.
 - a. You may make archival copies of the software files and you may modify and merge them into your software programs for the sole purpose of implementing the Product to protect and/or license your programs according to the Rainbow documentation provided with the Product. All software files remain Rainbow's exclusive property.
 - b. Rainbow's Sentinel System Driver Software and other Rainbow software files listed in the "Licensee Redistribution Allowances" section (if it is defined in the Product's documentation) may be copied and distributed to your customers for the sole purpose of executing your protected or licensed software programs according to the Rainbow documentation provided with the Product.
 - c. No license is granted to Licensee to sell, license, distribute, market or otherwise dispose of any software files or other component of the Product except when embedded in your software programs. Copies of your software programs must bear a valid copyright notice and must be distributed such that the object code for the Product cannot be extracted.
3. Rainbow warrants the Product and the magnetic media on which the software files are provided to be substantially free from significant defects in materials and workmanship under normal use for a period of twelve (12) months from the date of delivery of the Product to you. In the event of a claim under this warranty, Rainbow's sole obligation is to replace or repair, at Rainbow's option, any Product free of charge. Any replaced parts shall become Rainbow's property.
4. Warranty claims must be made in writing during the warranty period and within seven (7) days of the observation of the defect, accompanied by evidence satisfactory to Rainbow. Prior to returning any

Product to Rainbow, you must obtain a Return Material Authorization (RMA) number and shipping instructions from Rainbow. Products returned to Rainbow shall be shipped with freight and insurance paid.

5. Except as stated above, there is NO OTHER WARRANTY, REPRESENTATION, OR CONDITION REGARDING RAINBOW'S PRODUCTS, SERVICES, OR PERFORMANCE, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Rainbow is not responsible for any delays beyond its control. Rainbow's entire liability for damages to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of Product that caused the damages or that are the subject matter of, or are directly related to, the cause of action. In no event will Rainbow be liable for any damages caused by your failure to perform your obligations, or for any loss of data, profits, savings, or any other consequential and incidental damages, or for any claims by you based on any third-party claim.

Licensee Redistribution Allowances

SentinelSuperPro Licensees may release the Sentinel System Driver (sentinel.sys, sentinel.vxd) and the Sentinel Client Activator, as well as any associated files for installation with their SentinelSuperPro-protected application. In addition, the Licensee may distribute the following commands, files and related documentation: spcom-mon.dll, sp_g24.dll, sp_g08.dll, sp_g04.dll, makedll.dll, dsafedll.dll, dsafe32.dll, usafe32.dll, lang_enu.dll, fieldexutil.exe, fieldexutil.chm, licensegenutil.exe, licensegenutil.chm, makekeyutil.exe, makekeyutil.chm, instdrv.exe, instdrv.c, sentdata.vxd, monitor.exe, ssp_6_1_monitoring_tool.chm, loadserv.exe, spnsrvnt.exe, spnsrv9x.exe, the *SentinelSuperPro System Administrator's Guide* and Chapter 14 of the *SentinelSuperPro Developer's Guide*.

FCC Notice to Users

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment generates, uses, and can radiate frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If interference problems do occur, please consult the system equipment's owner's manual for suggestions. Some of these suggestions include relocation of the computer system away from the television or radio, or placing the computer AC power connection on a different circuit or outlet.

Change or modifications to this product without the express approval of Rainbow Technologies, Inc., could result in non-FCC compliance, and void the user's authority to operate this equipment.

International Quality Standard Certification



Rainbow Technologies, Inc. Irvine, CA facility has been issued the ISO 9002 Certification, the globally recognized standard for quality, by British Standards Institution as of December 1994.

Certificate Number FM 30128

European Community Directive Conformance Statement



This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC. Conformity is declared to the following applicable standards for electro-magnetic compatibility immunity and susceptibility; CISPR22 and IEC801. This product satisfies the CLASS B limits of EN 55022.

Contents

Preface

How to Get the Most from This Guide.....	ix
Accessing Online Documentation	x
<i>Using Online Help</i>	x
Accessing Printed Documentation	xi
Getting Help.....	xii
We Welcome Your Comments	xiv

Chapter 1 – What Is SentinelSuperPro?

SentinelSuperPro Components	2
<i>The Hardware Key</i>	2
<i>The SentinelSuperPro API</i>	4
<i>The SentinelSuperPro Developer’s Toolkit</i>	4
<i>The SentinelSuperPro Server</i>	5
<i>The SentinelSuperPro Monitoring Tool</i>	5
How SentinelSuperPro Protects Your Software	6
<i>Protection Types</i>	8
SentinelSuperPro Features and Benefits	10
<i>What’s New in SentinelSuperPro 6.1?</i>	14
What’s Included with SentinelSuperPro 6.1?	15
System Requirements.....	17
<i>Minimum Hardware Requirements</i>	17
<i>Minimum Software Requirements</i>	17

Chapter 2 – Installation

Running SentinelSuperPro Setup	20
<i>Preparing to Install</i>	20
<i>Installing SentinelSuperPro Components</i>	22
Installing the SentinelSuperPro Hardware Key	27
<i>Installing the Parallel Port Hardware Key</i>	28
<i>Installing the USB Hardware Key</i>	29

Chapter 3 – Protecting Your Applications

Step 1: Determine Which Applications to Protect	32
Step 2: Design Your Protection Strategy	32
Step 3: Open the Toolkit	38
<i>Navigating in the Toolkit</i>	39
<i>Using API Explorer and MemView</i>	40
<i>Creating a Project</i>	41
Step 4: Add Application Protection	42
Step 5: Add Custom Elements	43
<i>Types of Custom Elements</i>	43
Step 6: Create a Prototype	46
Step 7: Implement Your Protection Strategy	47
Step 8: Define Field Activation Actions	48
Step 9: Program Keys	50
Step 10: Ship Your Application	52
Step 11: Update Keys in the Field	53
<i>What Is a Locking Code?</i>	54
<i>What Is a License Code?</i>	54

Appendix A – Glossary..... 55

Preface

Thank you for selecting SentinelSuperPro to protect your applications from unauthorized use. The SentinelSuperPro software protection system combines a programmable hardware key with the ability to encrypt data, giving you a wide range of methods for securing up to 28 applications per key from illegal distribution and use.

How to Get the Most from This Guide

The *SentinelSuperPro 6.1 Quick Start Guide* walks you through installing the SentinelSuperPro Toolkit on your system, and introduces you to Sentinel software protection. The following table explains what you can find in each chapter of this guide:

Chapter/Appendix	Description
Chapter 1 – What Is SentinelSuperPro?	An overview of SentinelSuperPro components, features and benefits, including system requirements and what's new in 6.1.
Chapter 2 – Installation	Instructions for installing the Toolkit, the SentinelSuperPro server, the hardware key and the Sentinel driver.
Chapter 3 – Protecting Your Applications	Describes the steps required to protect your software using SentinelSuperPro, and provides information about where to go next.
Appendix A – Glossary	A glossary of SentinelSuperPro and software protection terms used throughout this guide.

Accessing Online Documentation

There are several ways to get help while using the SentinelSuperPro Developer's Toolkit (SSP Toolkit). For general issues, look for answers in this guide and in the online Help system that is included with the SSP Toolkit.

You may also want to read through the text provided in the SSP Toolkit's Overview stage. The introductory information included there can help you gain a basic understanding of SentinelSuperPro concepts.

Additionally, as you move through the stages, pay attention to the text that appears in the *orientation pane* at the top of the SSP Toolkit window. This text provides a quick overview of the steps you'll take in each stage and how they apply to protection strategies. If you find yourself unsure of what to do in a particular stage, read the orientation pane text for help.


Using Online Help

The SentinelSuperPro Developer's Toolkit ships with a complete online Help system. It includes a detailed table of contents and thorough index searching capabilities.

SSP Toolkit Help is very easy to use. The majority of the information found in this guide is also available through Help.

To access online Help, select **Help Topics** from the **Help** menu.

Most fields also have context-sensitive help associated with them, which is accessible in any of three ways:

- Right-click on a field, check box or button to view Help information specific to that item.
- Click in a field or on a check box, and then press **F1**.
- Click the **What's This** button  at the bottom of the SSP Toolkit window to access the Help pointer, then click on the item you need help for.

For more information, please review the Using Help topic in online Help.

Accessing SentinelSuperPro Documentation

If you can't find the answer you need in Help, refer to the SentinelSuperPro documentation for more detailed information and instructions.

Manual	What's In It?	Who Should Read It?
<i>SentinelSuperPro 6.1 Quick Start Guide</i>	A quick tour of SentinelSuperPro for Windows application developers.	Anyone who is new to SentinelSuperPro or software protection and wants a quick overview of SentinelSuperPro features.
<i>SentinelSuperPro 6.1 System Administrator's Guide</i>	Instructions for installing and running the SentinelSuperPro Server and Monitoring Tool.	Developers who will be implementing network functionality, and system administrators responsible for deploying a protected application in their organization.
<i>SentinelSuperPro 6.1 Developer's Guide</i>	All the steps necessary to protect, package and ship applications protected with SentinelSuperPro, as well as information about the SuperPro API calls.	Developers responsible for the overall process of protecting and shipping a Windows application.

Each of these guides are available in portable document format (PDF), and are installed on your computer during SentinelSuperPro setup.

You need Adobe Acrobat Reader to view and print PDF files. We recommend installing Acrobat Reader 4.0 or higher for best results. This version of Acrobat can be installed from the SentinelSuperPro CD.

Once you have installed Acrobat Reader, you are ready to access the documentation PDF files. To do so, navigate to **Start > Programs > Rainbow Technologies > SuperPro > 6.1**.

Tip: Check the Rainbow Technologies Web site (www.rainbow.com) for the most up-to-date versions of the SentinelSuperPro documentation.

Getting Help

Rainbow Technologies is committed to supporting SentinelSuperPro. If you have questions, need additional assistance, or encounter a problem, please contact Rainbow Technologies Technical Support using one of the methods listed in the following table:

Rainbow Technologies Technical Support Contact Information

Corporate Headquarters North America and South America	
	Rainbow Technologies North America
Internet	http://www.rainbow.com/support.html
E-mail	techsupport@rainbow.com
Telephone	(800) 959-9954 (6:00 a.m. – 6:00 p.m. PST)
Fax	(949) 753-9510
Australia	
	Rainbow Technologies (Australia) Pty Ltd.
E-mail	techsupport@au.rainbow.com
Telephone	(61) 3 9820 8900
Fax	(61) 3 9820 8711
China	
	Rainbow Information Technologies (China) Co.
E-mail	Sentinel@isecurity.com.cn
Telephone	(86) 10 8266 3936
Fax	(86) 10 8266 3948
France and Distributors in Europe, Middle East and Africa	
	Rainbow Technologies
E-mail	techsupport@fr.rainbow.com
Telephone	(33) 1 41.43.29.00
Fax	(33) 1 46.24.76.91

Rainbow Technologies Technical Support Contact Information (Continued)

Germany	
	Rainbow Technologies, GmbH
E-mail	techsupport@de.rainbow.com
Telephone	(49) 89 32 17 98 0
Fax	(49) 89 32 17 98 50
Taiwan	
	Rainbow Technologies (Taiwan) Co.
E-mail	techsupport@tw.rainbow.com
Telephone	(886) 2 2570-5522
Fax	(886) 2 2570-1988
United Kingdom and Ireland	
	Rainbow Technologies, Ltd.
E-mail	techsupport@uk.rainbow.com
Telephone	(44) 1932 579200
Fax	(44) 1932 570743

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

What Is SentinelSuperPro?

In addition to providing you with a full-featured, easy-to-use software protection system, SentinelSuperPro also gives you the ability to increase demo limits, upgrade demos to fully-licensed versions and provide access to additional features all without having to ship a new hardware key or visit the customer's site.

SentinelSuperPro 6.1 provides you with an added capability—the ability to allow your customers to use one key for multiple clients. SentinelSuperPro 6.1 also allows you to program keys specifically for use by your distributors, so you can limit how many product keys they can activate and update.

This chapter covers the following topics:

- SentinelSuperPro components
- How SentinelSuperPro protects your software
- SentinelSuperPro features and benefits
- What's new in SentinelSuperPro 6.1
- What's included with SentinelSuperPro 6.1
- System requirements for using SentinelSuperPro 6.1

SentinelSuperPro Components

The SentinelSuperPro system is made up of five components:

- The hardware key
- The SentinelSuperPro API
- The SentinelSuperPro Developer's Toolkit
- The SentinelSuperPro Server
- The SentinelSuperPro Monitoring Tool

Each of these components is explained in the following sections.

The Hardware Key

The SentinelSuperPro hardware key is a programmable, read/write memory device that provides the responses necessary to unlock your application. The hardware key is the heart of your application protection strategy.

To implement a protection scheme, you program your application to send calls to the hardware key to verify its presence. If the correct hardware key is attached to the user's system or available on the network, it responds to your application's calls with the appropriate responses, allowing the user access to your application.

Each key contains 64 memory cells, 56 of which are available for programming by you. These memory cells can be programmed with algorithms, data values to provide fixed responses, or to serve as counters. Each key also contains internal logic that transforms data based on encryption strings you define.

Stand-alone v. Network Keys

There are two types of SentinelSuperPro hardware keys: *stand-alone* and *network*:

- The *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 (see page 4), are programmed at the factory with a *hard limit*.

The hard limit defines the maximum number of licenses that can be obtained from the key, and thus the maximum number of users (both local and across the network) that can access the protected application. Keys are available with the following pre-programmed hard limits: 1, 2, 3, 5, 10, 25, 50 or unlimited.

- A *stand-alone key* is typically connected directly to a user's local workstation, providing access to the protected application only on a single system. Stand-alone keys have a hard limit of 0, meaning the key can be used by any number of local users. These keys can also be connected to servers, but provide only a single license at any one time.

Product Keys v. Distributor Keys

Prior to shipping your application to your customers, you must program your hardware keys with your protection strategy. A hardware key can be programmed as either a *product key* or a *distributor key*.

- *Product keys* are shipped to your end users with your protected application, providing access to the application. Product keys may be either stand-alone or network keys, depending on how your application will be used (by single clients or across the network).
- *Distributor keys* are given to your sales distributors, allowing them to perform activation and update functions on product keys provided to end users when they sell your protected application. Distributor keys can be either stand-alone or network keys; they must be connected to the distributor's local machine.

Rainbow Technologies customizes SentinelSuperPro hardware keys for each developer, which means another developer cannot reprogram your keys.

The SentinelSuperPro API

The SentinelSuperPro API is a set of functions used to communicate between your application, the Sentinel system driver, the server and the hardware key. If you choose to use the *integrated* protection option (see page 8), you embed API function calls to communicate with the hardware key directly in your application's source code.

The SentinelSuperPro Developer's Toolkit

The SentinelSuperPro Developer's Toolkit (SSP Toolkit) is a Windows application that combines the functions necessary to develop your protection strategy, program the hardware keys, and ship a protected application into one, easy-to-use package.

Once you have developed and prototyped your protection strategy using the SSP Toolkit, a protection plan with pseudocode is generated for you to use as a guide for adding the appropriate API function calls to your source code.

After you have modified your source code, or *shelled* your application (see page 9), you are ready to use the SSP Toolkit to program your hardware keys with the values your application will use to determine whether or not the key is attached to the user's system or the server.

The following SuperPro utilities from previous versions of SentinelSuperPro are now combined into the Developer's Toolkit:

- SentinelWizard
- SentinelShell
- SentinelSuperPro Advanced Editor
- SentinelSuperPro SAFE
- SentinelSuperPro Manufacturing Utility (SMU)
- Sentinel Evaluation Program

- Sentinel Query Response Generator

Tip: For more information about updating from SentinelSuperPro 5.1 or 6.0 to SentinelSuperPro 6.1, please refer to the SentinelSuperPro 6.1 Developer's Guide.

The SentinelSuperPro Server

If you design your protected application to be run on a network using concurrent licensing, your customer must install the SentinelSuperPro Server on the same machine where the hardware key is located. This server manages licensing and security for the protected application. The server is the link between the client running your application and the hardware key that responds to the API functions used in your protection strategy.

The SentinelSuperPro Monitoring Tool

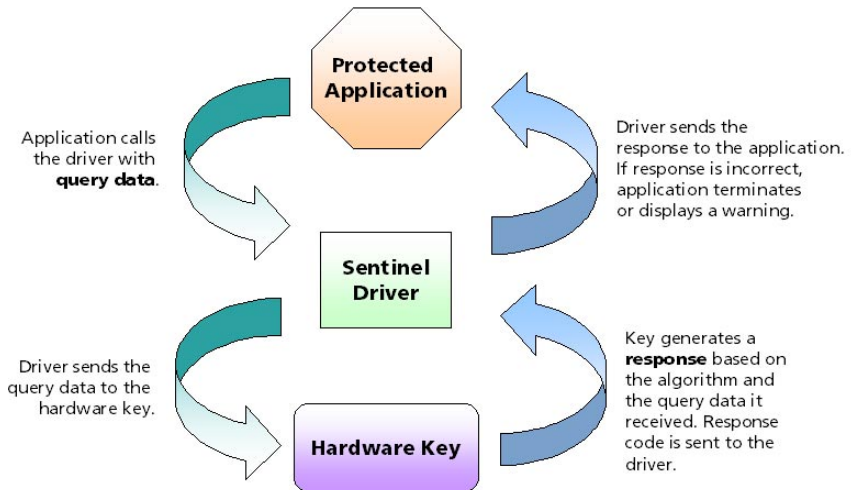
The SentinelSuperPro Monitoring Tool is a Windows application designed for use with protected applications intended to be run on a network. The Monitoring Tool displays information about all SentinelSuperPro servers, keys and user licenses in the field. The tool reports statistics, such as the number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

How SentinelSuperPro Protects Your Software

At its most basic, SentinelSuperPro protects your software through a series of steps known as a *software lock*. Each software lock is a call to an API function that verifies the presence of the hardware key to succeed.

1. Your application calls the Sentinel driver, which communicates with the hardware key attached to an external port on the user’s computer, sending a query string to an algorithm.
2. The key returns a response to the driver, which communicates back to your application.
3. Your application evaluates the response and acts accordingly.

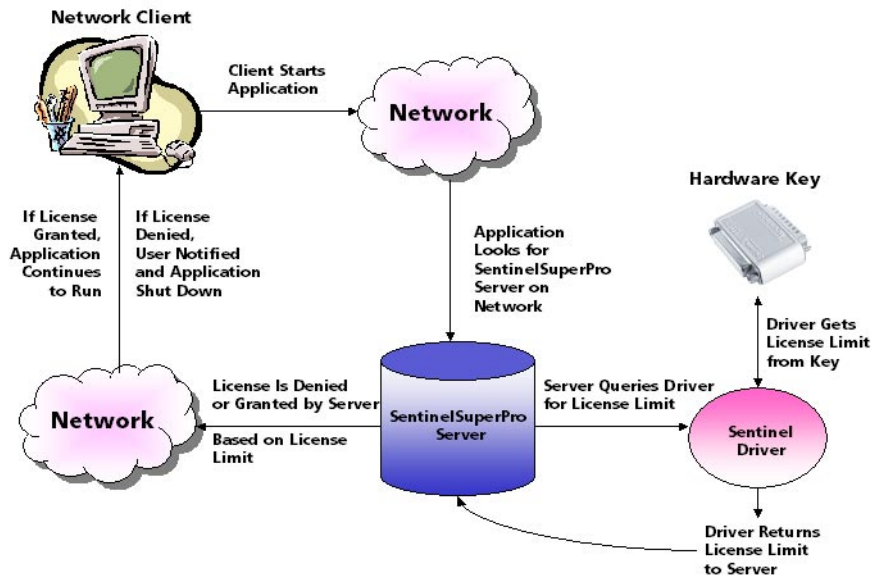
An invalid response indicates the correct key is *not* attached or has been tampered with. Your application then terminates or displays a warning message. Software can be illegally copied, but it will not run.



How the Key Handles Application Calls

When a SentinelSuperPro-protected application is used on a network, software locks are performed across the network only after a license has been obtained.

1. Your application sends a call to find a hardware key and obtain a license. If the key is found on the user's local system, software locks are performed as explained on page 6.
2. If a key is *not* found on the user's system, the application sends a broadcast message to the network to locate a SentinelSuperPro server.
3. Once found, the server queries the Sentinel driver to obtain the license limit from a hardware key attached to an external port on the server.
4. The driver reads the license limit in the key and returns it back to the server.
5. The server decides whether or not to grant the license and then sends the license information to your application.
6. After obtaining the license, your application sends periodic "heartbeat" messages to maintain the license. Failure to send a heartbeat message releases the license and returns an error to the application.
7. Software locks are performed as required by your application, using the license as permission to communicate with the key.
8. When all software locks are complete, the application releases the license back to the key through the server, allowing the license to be obtained by another client.



How an Application Obtains a License over the Network

Protection Types

SentinelSuperPro offers you two methods for protecting your application: *integrated* or *automatic*. When and where the software locks are implemented depends on the type of protection being used.

- **Integrated:** Integrated protection consists of software locks (API function calls) added directly to your source code. It is used to create a custom protection strategy, with control over the amount and location of software locks.

The frequency of software locks within your application, and the action taken if no key is found, is left up to you. The more locks you add to your application, the more difficult it will be for potential hackers to break your application's protection.

Because you must understand the API function calls used to support the protection strategy you have designed, and manually add them to your code, using integrated protection may take longer.

- **Automatic:** Automatic (*shelled*) protection is the fastest and easiest method of protecting your applications with SentinelSuperPro.

Instead of adding software locks to your source code, a protective “shell” is automatically added to your application’s executable file, so that the software lock is called before the application starts—if the hardware key is not present, the user sees an error message and the application does not run. Also, while the application is running, the shell periodically checks to verify the hardware key is still attached—if at any time the key is missing the application shuts down immediately.

Automatic protection also gives you more control over demo options such as expiration dates, counters and time/date limits.

SentinelSuperPro Features and Benefits

- **Customizable Protection**

One key can be programmed to provide several different types of both fixed and variable responses, giving you many variations in the types of software locks you can create.

For example, cells can be used to store fixed user data, such as serial numbers, user names or codes controlling feature access. Such data can be read by your application to verify the key is still attached or to perform some other function. You can also use stored data to control program flow or application functions.

Cells can also store algorithms used to scramble query codes sent by your application. Other cells can be programmed as counters used to restrict the number of executions. While the first eight cells are reserved for system information, the other 56 cells in each key can be used any way you desire (with some restrictions).

- **Password Protection**

The ability to program SentinelSuperPro hardware keys is protected by three passwords: the *write* password and two *overwrite* passwords. The write password allows you to write to undefined cells and read/write data words. The two overwrite passwords allow you to write to all other non-restricted cells: read-only data words, counters and algorithm words.

You must have your passwords to program keys through the SSP Toolkit or the Make Keys Utility. You also must include the passwords in your protected application to reprogram cells in the field or use some API function calls. Passwords ensure only authorized users can change your protection strategy or program keys.

- **Field Exchange Capability**

Shipping your protected application and its corresponding key(s) to customers in the field doesn't end your control over the key and your software. With SentinelSuperPro, you can perform a number of functions on keys already in the field, including activating and updating product, setting or clearing bits, and incrementing or decrementing counters.

Field exchange enables you to ship your application in an unusable state, and provide a means for legitimate users to activate it. The activation process is protected by encryption algorithms and passwords pre-programmed into the key. This same process also allows you to support field upgrades and control feature access.

- **Demo Application Control**

If you provide demo or trial versions of your applications to your customers, you may want those applications to run only a set number of times, or you may want to define an expiration date. SentinelSuperPro gives you demo application control through the use of counters, time limits and expiration dates.

- **Multiple Applications Per Key**

With SentinelSuperPro, you can protect up to 28 applications on a single hardware key. In each protection strategy, certain cells in the key are assigned to each application. Each application can then query the key using algorithms. Thus, your users can run several protected applications with a single hardware key attached.

The number of applications you can assign to a single key is dependent on how complex your protection strategy is. More complicated strategies require more memory cells, resulting in fewer cells available for other protected applications.

- **License Enforcement**

A significant addition to SentinelSuperPro 6.1 is its ability to enforce concurrent licensing agreements. The SentinelSuperPro server keeps track of the number of licenses in use for each key, and each sub-licensed application on the key, and does not grant new license requests once an application's license limit has been reached. When licenses are returned to the server by an application, they become available for reuse by another client.

The number of available licenses is determined by the hard limit programmed into the key, or through the use of sublicensing per application.

- **Sublicensing**

Sublicensing is useful when you want to apply a license limit that is less than the key's factory-programmed (*hard*) limit.

You can program up to 56 separate sublicense license limits in each key—each sublicense is a custom element occupying a single cell on the hardware key. The total number of sublicense limits you can program is dependent on the number of cells being used by other elements of your strategy.

In addition to defining your own license limits for the application as a whole, you can also use sublicenses to control concurrent access to specific features within a protected application. At runtime, access to a controlled feature is granted if the corresponding sublicense limit has not been exceeded.

- **Local or Network Access**

Using the SentinelSuperPro API, you can configure your application to run on a non-networked (*stand-alone*) system with a key directly attached, on a network using a license obtained from a key attached to a server, or on either a stand-alone system or a network, depending on how the application is being used.

- **Multiple Key and Server Support**

Up to 10 keys can be connected to parallel or USB ports on the same server; up to five parallel port keys can be attached to the same parallel port. There is no limit to the maximum number of servers you can have on the network.

Thus, the network's total concurrent license limit is the sum of all the limits in all keys attached to all servers. If a user attempts to access a protected application (assuming the application is running in the default *dual mode*), and the first server has reached its license limit, SentinelSuperPro automatically checks the first key on another server for an available license. Use of multiple servers helps avoid a single point of failure.

- **Application Time-Out**

The server can disconnect a user, and release the license for use by other users, after a pre-determined amount of time has elapsed without a SentinelSuperPro query or heartbeat message. This helps prevent idle users from tying up licenses, and permits recovery of licenses used by aborted programs or workstations that are unexpectedly disconnected from the network.

What's New in SentinelSuperPro 6.1?

SentinelSuperPro 6.1 improves upon SentinelSuperPro 5.1 by adding new features and updating existing features. These features include:

- Support for up to 28 protected applications per key*
- Network licensing capabilities allow for concurrent use of an application by multiple clients using a single key
- Integrated protection, key programming and activation functions in one application (the SSP Toolkit)*
- Enhanced user interface*
- Server monitoring tool allows system administrators to track license usage on the network
- Automatic cell allocation of elements*
- Ability to shell multiple applications on the same key*
- Addition of a one-time update option for license codes, allowing you to prevent a license code from being applied more than once during field exchange
- Activation actions/commands are automatically generated for applications that require activation*
- Unused cells can be skipped, randomized or cleared during key programming*
- Use of distributor keys provides developer control of the number of end-user keys distributors can activate and update
- Ability to override pre-programmed license limits through the use of sublicensing
- Integrated applications, shelled applications and custom elements can comfortably co-exist on the same key*

Note: Features marked with an asterisk (*) were originally available in SentinelSuperPro 6.0.

What's Included with SentinelSuperPro 6.1?

The SentinelSuperPro 6.1 package includes:

1. The SentinelSuperPro 6.1 CD, with the following software:
 - SentinelSuperPro 6.1 Developer's Toolkit
 - SentinelSuperPro 6.1 Server (*loadsrv.exe*, *spnsrv9x.exe*, *spnsrvNT.exe*)
 - SentinelSuperPro 6.1 Monitoring Tool (*monitor.exe*)
 - Sentinel system driver
 - Sentinel data protection driver
 - Make Keys Utility (*MakeKeysUtil.exe*)
 - License Generator Utility (*LicenseGenUtil.exe*)
 - Field Exchange Utility (*FieldExUtil.exe*)
 - Command-line shell utility (*ShellUtil.exe*)
 - Sentinel Client Activator
 - SentinelSuperPro merge modules for use with Windows Installer
 - SentinelSuperPro language interfaces
 - SentinelSuperPro documentation, including the *SentinelSuperPro 6.1 Developer's Guide* and the *SentinelSuperPro 6.1 System Administrator's Guide*.
 - Adobe Acrobat Reader (for accessing online documentation in PDF format)
2. One SentinelSuperPro hardware key

The type of key included in your package depends on whether you ordered a network or a stand-alone version of SentinelSuperPro. See the *SentinelSuperPro 6.1 Developer's Guide* for more information.

3. A document listing the passwords you need to program the key, including your developer ID, the write password and the overwrite passwords

Warning! *Your developer ID and passwords control access to your hardware key—do not lose them. If you do, you will need to return the key to Rainbow Technologies for a replacement. Also, to prevent unauthorized use of the key, be sure to keep the password document secure!*

4. This guide
5. Sentinel Client Activator documentation
6. A *readme.txt* file that provides late-breaking information about SentinelSuperPro, including system requirements, installation information and documentation updates (when necessary).

System Requirements

Review the following hardware and software system requirements prior to installing the SentinelSuperPro Developer's Toolkit.

Note: *System requirements for using the SentinelSuperPro Server and Monitoring Tool can be found in the SentinelSuperPro 6.1 System Administrator's Guide.*

Minimum Hardware Requirements

- Pentium microprocessor, P90
- VGA monitor (800 x 600 resolution recommended)
- 30 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
- 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 online Help file. This file **cannot** be viewed with any other browser, such as Netscape Communicator.*

Chapter 1 – What Is SentinelSuperPro?

Chapter 2

Installation

Before you can begin protecting your applications, you must install the SentinelSuperPro Developer's Toolkit, the SentinelSuperPro Server, the Sentinel system driver and the SentinelSuperPro hardware key.

Options for installing SentinelSuperPro client library interfaces, Visual C++ development tools and the SentinelSuperPro Monitoring Tool are also provided.

The following topics are covered in this chapter:

- Running SentinelSuperPro setup
- Installing the SentinelSuperPro hardware key

Tip: For information about installing SentinelSuperPro language interfaces or the Sentinel Client Activator, refer to the SentinelSuperPro 6.1 Developer's Guide.

Running SentinelSuperPro Setup

If you are installing SentinelSuperPro 6.1.1 on a Windows NT or 2000 workstation, you must have administrator-level access.

Before you begin installing SentinelSuperPro 6.1.1 components:

- **Save** and **Exit** out of all currently running applications.
- If you have SentinelSuperPro 6.1.0 installed, uninstall it. Versions 6.1.0 and 6.1.1 cannot co-exist on the same system.

Note: *If you have SentinelSuperPro 5.1 or 6.0 installed on your system, you do not need to uninstall it before you begin this procedure. SentinelSuperPro 6.1.1 can co-exist on the same system as 5.1 or 6.0 without any problems.*

- Disconnect all SentinelSuperPro USB hardware keys from your system.
- Verify that you have Internet Explorer (IE) 4.x or higher installed on your system.

Setup will not run if IE 4.x or higher is not installed; to install the latest version of IE, go to <http://www.microsoft.com>.

Internet Explorer is used to view SentinelSuperPro HTML Help. It must be installed prior to setup so that additional components required to view HTML Help files can be installed.

Preparing to Install

1. Place the SentinelSuperPro 6.1.1 CD in your CD-ROM drive.

The setup program should start automatically. If not, navigate to the following path (assuming E: is the drive letter of your CD-ROM drive): *E:\Start.exe*, and then double-click on the file.

The SentinelSuperPro installation screen appears.

Note: *If you have problems accessing the SentinelSuperPro installation screen, you can start the setup program manually by navigating to the following path: E:\SentinelSuperPro6.1.exe, and then double-clicking on the file.*

2. Click **SentinelSuperPro 6.1 Developer's Toolkit**. A status bar appears while setup prepares to start the installation process.
3. Do one of the following:
 - If this is the first time you have run the Windows Installer program on this system, a message box prompting you to reboot your system may appear. If so, you must restart your system to continue the installation. Click **Restart**, then go to step 4.
 - If the above message box does not appear, go to step 5.
4. Once your system has completed rebooting, SentinelSuperPro setup should resume automatically. If it does not, double-click the setup file again to restart the installation process.
5. After the file is unpacked, do one of the following:
 - If the Sentinel Driver Upgrade screen appears, go to step 6.
 - If the SentinelSuperPro Welcome screen appears, go to step 1 of “Installing SentinelSuperPro Components” on page 22.
6. If you already have a previous version of the Sentinel driver installed, the Driver Upgrade screen appears. You *must* upgrade to the latest version of the Sentinel driver to use SentinelSuperPro 6.1. Read the on-screen message, then click **Upgrade**.

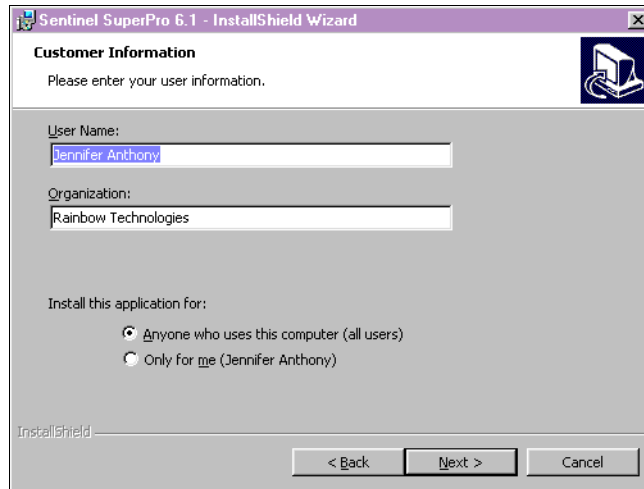
Installing SentinelSuperPro Components

After the setup program has verified your system has the appropriate installer files and has checked for an existing Sentinel driver, you are ready to start installing SentinelSuperPro. The SentinelSuperPro Welcome screen appears.

1. After reading the preliminary information, click **Next**. The license information appears.
2. To accept the license and continue, select the **I accept the terms in the license agreement** option, then click **Next**.

The Next button is not available until you select the “I accept” option.

The following screen appears:



Customer Information Screen

3. Enter or verify your user name and organization name in the appropriate fields.
4. Select who you want this application to be installed for.

- To allow anyone who logs on to this system to be able to run SentinelSuperPro, select **Anyone who uses this computer (All users)**.
- To make SentinelSuperPro accessible only when you are logged on to this system, select **Only for me (your name)**.

To increase the security of your application protection strategies, you may want to prevent other users from being able to run the SentinelSuperPro Toolkit by selecting **Only for me**. However, if more than one user will need access to SentinelSuperPro on this system, be sure to select **Anyone who uses this computer**.

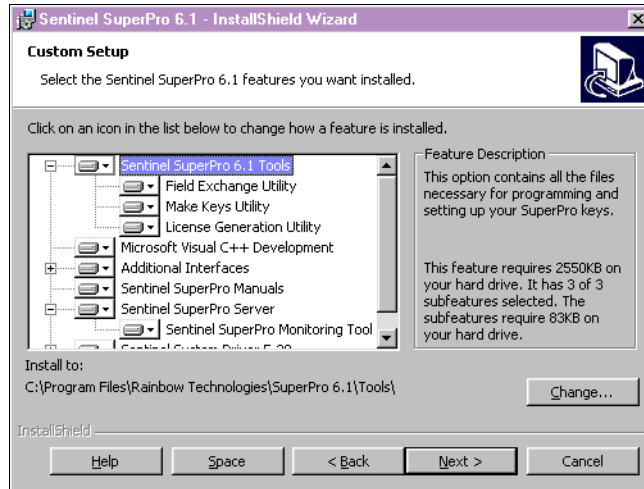
5. Click **Next**. The Setup Type screen appears.
6. Select one of the following:
 - **Complete**: Installs all SentinelSuperPro components, including the SentinelSuperPro 6.1 Developer's Toolkit, the SentinelSuperPro Server, the SentinelSuperPro Monitoring Tool, the SentinelSuperPro documentation, and other supporting files and utilities.

A complete installation requires 35 MB of free disk space.

Note: *You cannot change the default installation location of C:\Program Files\Rainbow Technologies\SuperPro\6.1 when you select Complete. To change the installation location, select **Custom**.*

- **Custom**: Allows you to select which components you want to install, and to change the default installation location for each component.

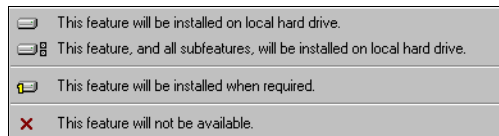
If you selected **Complete**, go to step 13. If you selected **Custom**, the list of SentinelSuperPro components appears. Go to the next step.



Custom Setup Screen – List of Components


Note: *If this is your first time running the setup program, you must install **SentinelSuperPro 6.1 Toolkit**, **SentinelSuperPro Server** and **Sentinel System Driver 5.39**.*

7. By default, all components are marked for installation. To select which components will not be installed, click the component’s icon . A shortcut menu appears.



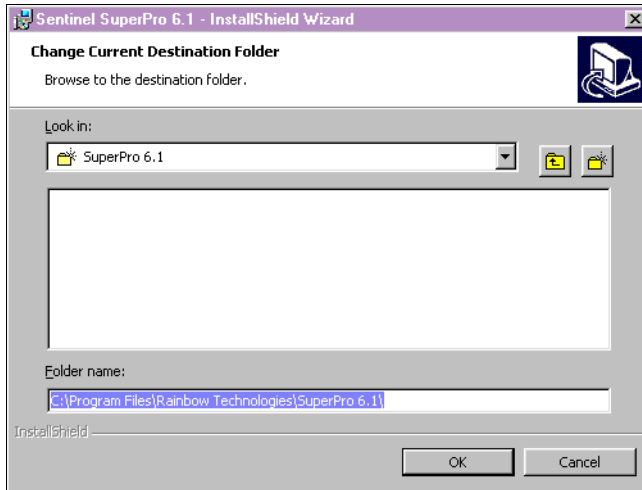
Install Options Shortcut Menu

8. From the shortcut menu, select the appropriate option.

For example, to prevent a component from being installed, select **This feature will not be available**. An  appears in place of the component’s icon.

Note: If a **+** is located to the left of a component's icon, that component has subcomponents that can be selected for installation separately. Click the **+** to view the available subcomponents.

- To change the location where SentinelSuperPro components will be installed, select a component, then click **Change**. The Change Current Destination Folder screen appears.



Change Current Destination Folder Screen

- To change the default location for the selected component, browse to select a new folder, then click **OK**.
- Repeat steps 9 and 10 for each component you want to change the installation location for.

Note: *You should always install the SentinelSuperPro Server on a local hard drive. Do not install the server on a network drive. If you install the server on a network drive, you will be unable to start it, and thus unable to use SentinelSuperPro.*

12. Once you have selected which components you want to install, click **Next**.
13. When the Ready to Install screen appears, click **Install**. SentinelSuperPro begins installing on your system. Once installation has finished, an “install complete” screen appears.

Note: *Depending on your operating system, you may need to reboot your system at this point. You will be prompted if a reboot is required; if a message appears, follow the on-screen instructions.*

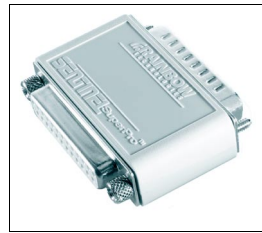
14. Click **Finish**, then go to the next section to install the SentinelSuperPro hardware key.

Installing the SentinelSuperPro Hardware Key

SentinelSuperPro comes with one hardware key for you to use while you are designing and implementing your application protection strategies. The key must be connected to your workstation while you run SentinelSuperPro software.

When you placed your order for SentinelSuperPro, you should have specified whether you wanted a network version, or a non-network version. The type of key you receive—network or stand-alone—depends on the version of SentinelSuperPro you ordered. Network keys 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*. Again, 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: For instructions on installing SentinelSuperPro hardware keys on a server, please refer to the SentinelSuperPro System Administrator’s Guide, included in your package.

Installing the Parallel Port Hardware Key

The SentinelSuperPro key can be attached to any parallel port on your computer, as the Sentinel driver automatically polls each port to locate the key.

1. Locate an available parallel port on your computer.

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 (Rainbow Technologies p/n 103027-001).*

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.

Installing the USB Hardware Key

If you have multiple USB ports (if, for example, you are using a USB hub), you can connect up to 10 USB hardware keys on a single computer. Cascading—connecting multiple keys to the same port—is not supported for SentinelSuperPro USB hardware keys.

We recommend installing the Sentinel system driver prior to connecting any USB keys to your system.

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

Chapter 2 – Installation

Chapter 3

Protecting Your Applications

To protect your applications with the SentinelSuperPro Toolkit, you need to follow a simple series of steps, which are outlined in this chapter.

If you have used previous versions of SentinelSuperPro, and are already familiar with the concepts used (such as the use of algorithms, counters and data words, and the use of activation types), this chapter should allow you to familiarize yourself with this new version and quickly start protecting your applications, without any additional training.

If you are new to SentinelSuperPro, use this chapter as a jumping off point for using the SentinelSuperPro Toolkit. The information in this chapter is designed to give you an overview of the steps involved in protecting applications. In-depth discussions of Sentinel protection concepts and techniques, as well as detailed procedures for using the Toolkit, are provided in the *SentinelSuperPro 6.1 Developer's Guide*, which we recommend you read before you begin protecting your applications.

The following steps are used to protect an application using the SentinelSuperPro Developer's Toolkit:

Step 1: Determine Which Applications to Protect

You can protect up to 28 applications on a single key using SentinelSuperPro. The number of applications is dependent on the number of elements you have programmed on the key. The more elements you have, the more memory cells that are used, and thus the fewer applications you can protect.

Step 2: Design Your Protection Strategy

When you design your protection strategy, you decide what types of protection you are going to use for your applications, which activation types you need, and how you are going to implement the protection in your source code. Ask yourself the following questions:

- **Will I use *integrated protection* or *automatic protection*?**

When you choose *integrated protection*, you add software locks—API functions to verify the presence of the key—directly into your application’s source code.

Integrated protection is most commonly used when you want to have control over the protection techniques used to secure your application and you have access to the source code and understand the API functions.

When you use *automatic protection*, SentinelSuperPro wraps a protective layer, called a *shell*, around your application’s executable file. This layer is encrypted, making it more difficult for a hacker to gain access to your application’s code. The shell layer makes no changes to your application’s source code.

Automatic protection is most desirable when you don’t have access to the application’s source code and/or you don’t have the time or desire to design a unique protection scheme.

- **Will my application be *active* or *inactive*? Will it be a *demo*?**

An *active application* is one that is ready to run when shipped to your customer. It will always remain active, as long as the hardware key is attached.

An *inactive application* will not run until it is activated by the user entering an activation password.

A *demo* is a trial version of an application that uses a counter to control the number of times the application can be run before it expires. Demo or metered applications are shipped as active, but usually become inactive after a specific number of executions.

- **Will my application be a *stand-alone* or *network* application?**

Another decision you need to make while protecting your application is how you want to use *licenses* with your application. With Sentinel-SuperPro 6.1, every user of your application needs to obtain a license before he can run the application. The license allows the user to start the application and access the hardware key.

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.

Licenses can be used in two ways—with a *stand-alone* application or with a *network* application. If the application is stand-alone, each user needs his own hardware key, as only one license can be obtained from each key. If the application is a network application, only one key—located on the network—is required, but the single key can issue multiple licenses, allowing for simultaneous use of your application by several clients.

The type of licensing model to use is up to you. It depends on how you will be selling your application, and how you expect your users to deploy it within their organization.

- **Will I use *sublicensing*?**

Sublicensing is useful when you want to apply a license limit that is less than the key's factory-programmed (hard) limit. Typically, sublicenses are used only with network applications.

In addition to defining your own license limits for the application as a whole, you can also use sublicenses to control concurrent access to specific features within a protected application. At runtime, access to a controlled feature is granted if the corresponding sublicense limit has not been exceeded.

- **What *activation type* will I use?**

The methods defining how customers activate your application are called *activation types*. There are four activation types in SentinelSuperPro: *active*, *static*, *trusted* and *distributed*.

The table on the following page describes each of the available activation types, what you must do to use each type, and suggestions for how you can use each type. Typically, the activation type you use is based on whether you want your application to be active or inactive.

SentinelSuperPro Activation Types

Activation Type	Description	When to Use
Active	<ul style="list-style-type: none"> Your application is always active when the hardware key is attached. It needs no activation password. 	<ul style="list-style-type: none"> You want your main product to be always active so your customer can always run it. You might ship add-on features (that you intend to charge separately for) as inactive products, to be activated at a later time when your customer purchases them.
Static	<ul style="list-style-type: none"> The application is <i>inactive</i> until activated with an activation password, unless it is a demo or metered application. The activation password is the same for every hardware key used to protect the application. This means one password works for multiple keys. 	<ul style="list-style-type: none"> This type is easier to deploy, because the password is always the same, making it easier to update several keys on different computers. If you are writing a separate activation password utility, you must use this type because you know what the password will be.
Trusted	<ul style="list-style-type: none"> The application is <i>inactive</i> until activated with an activation password, unless it is a demo or metered application. Activation passwords are generated by SentinelSuperPro and are unique for each hardware key and each application. Requires distribution of the Field Exchange Utility or the Sentinel Client Activator for field activation. 	<ul style="list-style-type: none"> Provides excellent security, because all passwords are unique. Best for use with applications using automatic (shelled) protection. You cannot use this type when you are writing your own activation password utility, because you never know what the password for a specific key will be.

SentinelSuperPro Activation Types (Continued)

Activation Type	Description	When to Use
Distributed	<ul style="list-style-type: none"> • The application is <i>inactive</i> until activated by a product distributor, unless it is a demo or metered application. • Activation passwords are generated by SentinelSuperPro and are unique for each hardware key and each application. • Distributor uses the Field Exchange Utility or Sentinel Client Activator to activate the application. Each activation decrements the distributor key's counter. • Requires programming and distribution of a distributor key in addition to the product keys. 	<ul style="list-style-type: none"> • Must be used if you want to keep track of the number of product activations performed by your distributors. • If you want to charge your distributors for product activations. The distributor key keeps track of the number of activations, and when the counter reaches zero, no more activations are allowed. You can update (and charge for) a distributor key with more activations in the same way that product keys are updated.

As you design your protection strategy, you should also keep in mind the following basic protection guidelines:

- **Send Frequent Queries**

One of the most basic and effective techniques you can use to confuse hackers is to call the hardware key frequently. If you rely on a single call at the beginning of your code, it is relatively easy for a skilled hacker to isolate the call and defeat your protection.

Another potential problem with querying only once is that a user could remove the key after starting the application. The key could then be used to run another copy of the application. The first copy would continue to run, because no queries are being performed to check for the key's continued presence.

This process of removing a key after starting an application and then using the same key to start the application on other computers is known as “lamplighting.”

If you decide to implement network licensing as part of your protection strategy, you must send a message to the key every 90 seconds in order to maintain the license. Failure to send this “heartbeat” message to the server (and thus the hardware key) will result in loss of the license and an error being sent to the application. Heartbeat messages let the server and key know that the license is still in use by the client running the application.

- **Scatter Lock Code**

Software locks consist of multiple steps: calling the key, evaluating the returned value, and acting on the evaluation results. For added protection, separate these lock components in your code. A software lock is harder to break if its code components are physically separated into different sections of the application instead of being located together.

- **Manipulate Returned Data**

Use the data returned from the hardware key in various ways. For example, leave the result in a variable, then check it later.

Tip: For detailed information about designing a protection strategy, see Chapters 4 and 5 of the SentinelSuperPro 6.1 Developer’s Guide.

Step 3: Open the Toolkit

The SentinelSuperPro Server must be running in order for the Toolkit to be able to access the hardware key while you create your protection strategy. Therefore, before starting the Toolkit, verify you have the server running on your system. See the *SentinelSuperPro System Administrator's Guide* for more information about using the server.

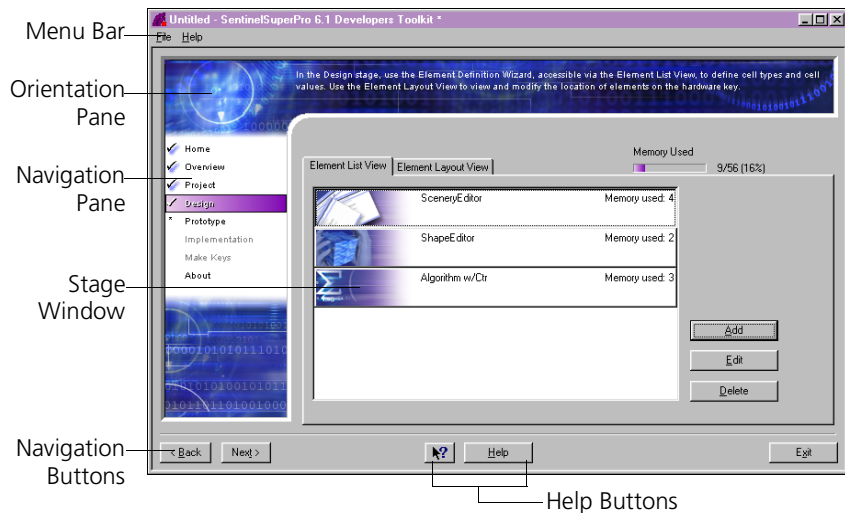
To open the SSP Toolkit:

1. From the **Start** menu, point to **Programs > Rainbow Technologies > SuperPro > 6.1**.
2. Select **SuperPro 6.1 Toolkit**. The Developer Configuration dialog box appears.

Before you can use SentinelSuperPro, you must provide your **developer ID**, **overwrite passwords** and **write password**. These passwords, and your developer ID, are provided by Rainbow Technologies, and can be found on the password sheet included in your SentinelSuperPro package.

Refer to the *SentinelSuperPro 6.1 Developer's Guide* for detailed instructions on entering your passwords and choosing options in the Developer Configuration dialog box.

Navigating in the Toolkit



Toolkit Window (with Design Stage Open)

The SSP Toolkit is made up of eight different *stages*. Stages appear in the *stage window*, where sections and sub-sections within the window help you navigate to the tasks necessary to implement your protection strategy. The stages are as follows:

- **Home** – The default stage that appears when the SSP Toolkit opens. No tasks are performed in this stage.
- **Overview** – Sections in this stage introduce you to SentinelSuperPro concepts. This stage also features the API Explorer, where you can test API function calls, view the key's cell layout, and send queries to the key to obtain return values.
- **Project** – This stage provides setup and configuration information. Create or open projects and enter your developer ID and passwords in this stage.

- **Design** – The Design stage has two sections: Element List View and Element Layout View. Use the Element Definition Wizard, accessible via Element List View, to define cell types and cell values. Element Layout View allows you to view and modify the location of algorithm, counter and data word cells on the hardware key.
- **Prototype** – In this stage, you program the cells in the hardware key with the values defined in the Design stage, generating pseudocode for use in adding API functions to your source code. *This stage is a required stage.*
- **Implementation** – When you implement your strategy, you add the appropriate protection to your application code, either by adding a shell to the application's executable file, or adding API functions to the source code based on the pseudocode generated during prototyping. This stage also allows you to define the actions that can be taken through field activation, and is used to create license codes for distribution to customers who have purchased upgrades in the field.
- **Make Keys** – Hardware keys programmed with your protection strategy, as defined in the Design stage, must be distributed with each copy of your software. The Make Keys stage allows you to program keys prior to distribution.
- **About** – For more information about the version of the SSP Toolkit you are using, or links to Rainbow Technologies information on the Web, go to this stage. No tasks are performed in this stage.

Using API Explorer and MemView

There are two utilities within the SSP Toolkit you should become familiar with, as you will use them quite often while protecting your applications:

- The *API Explorer* allows you to experiment with API function calls on various cells in the key before you add them to your source code. It is also a good way to familiarize yourself with the available functions and their uses prior to designing your strategy.
- The *MemView* section of the API Explorer provides a graphical view of the address, access code and value for each cell on the attached key.

Both of these utilities are available in the Overview and Implementation stages.

Creating a Project

A project is stored in a SentinelSuperPro Toolkit file. The project contains all the data used to create your protection strategy—elements, passwords, your developer ID, algorithm values, counters, data words, field activation commands, etc.

Your project is the template that will be used to program the keys protecting your application.

When you open the SSP Toolkit, a new project, *untitled.spp*, is created by default. We recommend saving this project with a more meaningful name before starting to design your protection strategy.

Tip: For detailed information about opening and navigating in the Toolkit, using API Explorer and MemView and creating a project, see Chapter 6 of the SentinelSuperPro 6.1 Developer's Guide.

Step 4: Add Application Protection

The first step in applying application protection is to select whether you want to use automatic or integrated protection. The Element Definition Wizard walks you through the process of adding protection to your application.

To access the Element Definition Wizard:

1. Navigate to the **Design** stage.
2. Verify you are on the **Element List View** tab.
3. Click **Add** to start the Element Definition Wizard. You are asked to select the type of element you want to add.
4. Select **Application Protection**, then click **Next**.
5. Select **Integrated** or **Automatic**, then click **Next**.

The Element Definition Wizard continues, prompting you to select options that apply to the type of protection you selected in step 5.

Tip: For detailed information about adding application protection, see Chapter 7 of the Sentinel-SuperPro 6.1 Developer's Guide.

Step 5: Add Custom Elements

In addition to adding application protection to your protection strategy, you can also add individual design elements, such as algorithms with counters and passwords, individual counters, and data words that contain data you want to store on the key, such as serial numbers or user data.

These elements are optional, and are necessary only if you need them to implement your custom protection strategy.

Custom elements are added to your strategy through the Element Definition Wizard, similar to how you added application protection to your strategy.

Types of Custom Elements

There are several types of custom elements you can add, depending on what you want to do. The following table describes each element.

Custom Element Types

Element Type	Cells	Description	Use If You Want To...
Algorithm	2	A simple algorithm.	Scramble an input string but do not want an associated counter or activation password.
Algorithm with counter	3	An algorithm with an associated counter.	Limit the number of times a demo program can be executed.
Algorithm with password	4	An algorithm that has a password associated with it.	Have the user enter a password to make the application run initially.

Custom Element Types (Continued)

Element Type	Cells	Description	Use If You Want To...
Algorithm with counter and password	5	An algorithm that has both a counter and a password associated with it. The algorithm is deactivated when the counter reaches zero. The user must enter a password to reactivate it after the counter reaches zero.	Limit the number of times a demo application can be executed and provide a means for the program to be re-activated in the field.
Algorithm with 2 counters	4	An algorithm that has two counters associated with it.	Use two counters. The first counter that reaches zero deactivates the algorithm, which usually stops your application from executing properly.
Algorithm with 2 counters and 1 password	6	An algorithm that has two counters and a password.	Implement an algorithm that is to be deactivated when either counter reaches zero. The user must enter a password to activate or reactivate the application.
Counter	1	A cell that contains a value you can decrement.	Limit the number of times a demo program can be run, or count the number of times any particular operation is performed.

Custom Element Types (Continued)

Element Type	Cells	Description	Use If You Want To...
User data	1	A cell that contains a value your application can test (and change) during execution. If the cell is locked, the value is read-only; your application can read the stored data but cannot change it without the overwrite passwords.	Store a serial number, feature control code or other data you define.
Sublicense	1	A cell that contains a value you select as a sublicense limit.	Restrict the license limit for this application to something less than the hard limit already programmed into the key.

Note: For more information on when to use custom elements, refer to Chapter 4 of the Sentinel-SuperPro 6.1 Developer's Guide. For detailed instructions on adding custom elements, see Chapter 8 of the same guide.

Step 6: Create a Prototype

The first step in implementing your strategy is to create a *prototype* hardware key. When you create a prototype of your protection strategy, you are actually programming a master key with all of the elements you previously defined as part of your protection strategy.

Creating a prototype is a **required** step.

During prototyping, after the key is programmed, SentinelSuperPro also performs the following functions:

- **Generates query/response pairs for each application included in your strategy.** Queries are used to verify the presence of the key while your application is running.
- **Defines default field activation actions and commands.** If any of the applications or custom element algorithms in your strategy use the activation type Static, Trusted or Distributed, SentinelSuperPro creates a default action and command for activating the application in the field.
- **Generates a pseudocode protection plan.** The pseudocode protection plan outlines the API functions you need to add to your application (if you are using integrated protection), as well as additional information about your protection strategy.

Tip: For more information on creating a prototype, refer to Chapter 9 of the SentinelSuperPro 6.1 Developer's Guide.

Step 7: Implement Your Protection Strategy

When the prototype is complete, you are ready to implement your strategy. To do so, navigate to the Implementation stage in the SSP Toolkit.

If you are using integrated protection for your application, you must manually add the appropriate API function calls to your application's source code in order to implement your protection strategy. The SSP Toolkit provides you with pseudocode that tells you what functions you need to add to your code—click the **Integrated Apps** tab to view the pseudocode.

To add API function calls to your application code, look at the example code provided for your development language. This code is available from the SentinelSuperPro installation Web site. The example file shows the exact syntax for each SentinelSuperPro API function.

Applications you have defined as using automatic (“shelled”) protection are easy to implement, as all you need to do is click a button to add the protective shell layer to your executable file. Once the shell has been added, all the protection options you defined for the application are in place.

Tip: *For more information on adding API calls to source code and adding a shell to an application, refer to Chapter 9 of the SentinelSuperPro 6.1 Developer's Guide.*

Step 8: Define Field Activation Actions

To be able to update keys in the field, you need to define the field activation actions and commands that can be performed on keys using your protection strategy.

Commands are API function calls that describe what will be done to the key in the field. For example, the Decrement Counter command locates the counter cell on the key and decrements it by the value you specify. Actions are groups of one or more commands.

The following commands are available for field activation:

Command	Description
Write Cell	Writes the value you entered to the selected cell.
Activate Algo PW1	Enables an inactive algorithm already on the key. The value you enter is passed as a parameter to the ActivateAlgorithm function. This command must be used in conjunction with the Activate Algo PW2 command.
Activate Algo PW2	Enables an inactive algorithm already on the key. The value you enter is passed as a parameter to the ActivateAlgorithm function. This command must be used in conjunction with the Activate Algo PW1 command.
Decrement Counter	Decrements a counter cell. This command reads the current counter value and then subtracts one from the value.
Increment Distributor Counter	Increments the activation counter cell on a distributor key. This command reads the current counter value and then adds the value you specified. This command is available only if you have a distributed application included in your protection strategy.

Command	Description
Increment Counter	Increments a counter cell. This command reads the current counter value and then adds the value you specified.
Bit Mask AND	Used to clear a bit in a cell value.
Bit Mask OR	Used to set a bit in a cell value.
Decrement Counter to Zero	Decrements a counter cell to zero, regardless of the current value. Typically used when you are updating a demo to a fully-licensed version; must be used in conjunction with other commands.

Note: For more information on adding field activation actions and commands, refer to Chapter 10 of the SentinelSuperPro 6.1 Developer's Guide.

Step 9: Program Keys

Once you have completed your protection strategy, including prototyping a master key, you are ready to start programming product keys to include in the final package with your protected application, and distributor keys to send to your distributors.

To program a product key:

1. In the SSP Toolkit, open the SentinelSuperPro project containing the protection strategy for the application you are programming a key for.
2. Navigate to the **Make Keys** stage. A list of the applications you applied integrated or automatic protection to appears.
3. Connect the key you want to program to the appropriate port on your workstation.
4. Click **Program Key**. The key is programmed with the protection strategy you defined.
5. If the programming was successful, disconnect the key from the port.

To program a distributor key:

1. In the SSP Toolkit, open the SentinelSuperPro project containing the protection strategy for the application you are programming a key for.
2. Navigate to the **Make Keys** stage.
3. Click the **Distributor Keys** tab.

A list of the applications you applied integrated or automatic protection to, *and* assigned the Distributed activation type to, appears. You can program distributor keys *only* for those applications using the Distributed activation type.

4. Connect the key you want to program to the appropriate port on your workstation.
5. In the **Distributed Applications** list, select the check box for the application you want to assign metering options for.
6. Under **Metering Options**, select one of the following:
 - **Unlimited:** To allow the distributor to activate or update as many of your products as they like.
 - **Limited:** To pre-define the number of applications the distributor can activate or update. Enter a number in the corresponding field.
7. Repeat steps 5 and 6 for each application you want the distributor to be able to activate and update.

You can program a distributor key to activate or update multiple applications. When you select the check box for the next application, the metering option changes to the default value of zero, or to the value you previously selected for the application.

8. Click **Program Key**.

The key is programmed with the protection strategy you defined.
9. If the programming was successful, disconnect the key from the port.

Tip: For more information on programming keys, refer to Chapter 11 of the SentinelSuperPro 6.1 Developer's Guide.

Step 10: Ship Your Application

When your application is complete, and your product keys are programmed, you are ready to ship your protected application to your distributors and/or customers.

What you ship depends on who you are sending the application to. Customers usually only need the application, the key and the Sentinel driver.

However, when you ship your application to distributors, there are additional items you must ship along with your application and the product key, such as the distributor key and the stand-alone utilities used for field activation or key programming.

For complete lists of what to send to customers and distributors, please refer to Chapter 12 of the *SentinelSuperPro 6.1 Developer's Guide*.

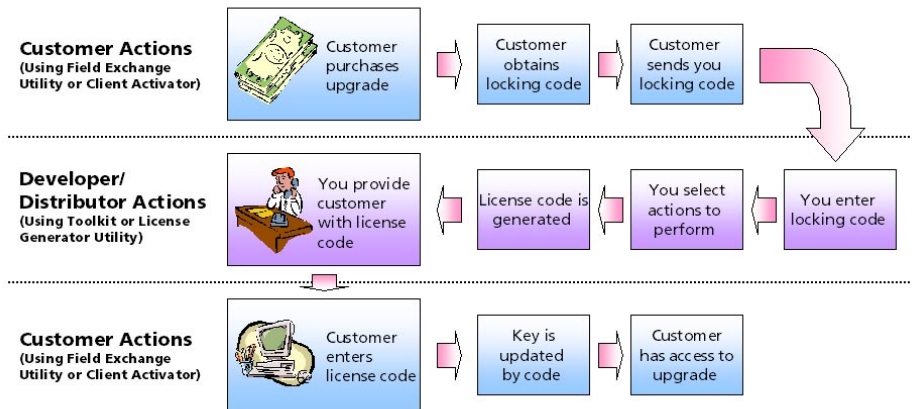
Step 11: Update Keys in the Field

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

In the field, your customers generate a *locking code* that they send to you. You then input the locking code in the Field Activation section of the Implementation stage to generate a *license code* that you return to the customer. The license code updates the key and activates the customer's application appropriately.

SentinelSuperPro keys in the field are updated remotely as a result of information exchanged between you and your customer. 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 Developer/Distributor Roles in Key Activating or Updating

Field activation requires both you (or your distributor) and your customer to exchange information about the key. Your customer is responsible for generating and sending the locking code to you. You (or your distributor) are responsible for generating and sending the license code to the customer.

What Is a Locking Code?

The locking code for a key includes information about how the key is currently programmed, including the key's serial number and developer ID. You must have a customer-generated locking code to create a license code.

Locking codes are unique for each key. In previous versions of SentinelSuperPro, the locking code was known as the Key ID string.

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 activated or updated; for example, what new features the customer 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 provided by the customer and the actions you select.

License codes are unique to the key the locking code was generated from. In previous versions of SentinelSuperPro, the license code was known as the Update Key string.

Tip: For more information about updating keys in the field, including how distributors update or activate keys, please refer to Chapter 13 of the SentinelSuperPro 6.1 Developer's Guide.

Appendix A

Glossary

A

- access code** An attribute that identifies the accessibility and functionality of a cell. Possible values are:
- 0 read/write data word
 - 1 read-only (locked) data word
 - 2 counter
 - 3 algorithm/hidden
- See also* **locked word, hidden word, data word, counter, algorithm.**
- access mode** Access modes determine where your application will look for the appropriate hardware key. There are three access modes that can be used by your protected application: *stand-alone, network* and *dual*. *See also* **network mode, dual mode, stand-alone mode.**
- action** A group of one or more field activation commands. *See also* **field activation, command.**

activation password	<p>A two-word value that can be used to activate an inactive algorithm. The password is programmed into the two cells immediately following the algorithm. You give your users the password and a utility with which to enter it.</p> <p>Activation passwords use access code 3. They are called hidden words because their values cannot be read by your application. <i>See also</i> access code, algorithm, hidden word.</p>
activation type	<p>Protection provided by SentinelSuperPro that allows for various methods of customer activation of program modules. Possible activation types are <i>active, static</i> and <i>trusted</i>. <i>See also</i> active activation type, static activation type, trusted activation type.</p>
active/inactive bit	<p>A bit in an algorithm's second word that controls whether or not the algorithm will respond correctly to a query. An algorithm must be active to respond to a query. <i>See also</i> algorithm, query.</p>
active activation type	<p>Method of activation provided by SentinelSuperPro where the application is always active. It does not need an activation password (no activation is necessary).</p> <p><i>See also</i> activation type, activation password.</p>
active application	<p>An application that is ready to run when shipped to your customer. It will always remain active, as long as the hardware key is attached.</p>
address	<p>The memory used to identify a specific cell. <i>See also</i> cell.</p>
algorithm	<p>An element containing a bit pattern that defines how the hardware key should encrypt query data sent by your application. The key uses an algorithm to encrypt the query data and then return a value to your application. You design your application to send queries to the key and then evaluate and act upon the responses.</p>

Algorithms can be *active* or *inactive*. Only active algorithms can return a valid response to a query. The *active/inactive bit* in the cell value controls whether or not the algorithm is active.

All algorithms are two words (and thus, two cells) long, and may have activation passwords and counters associated with them.

See also **query data, active/inactive bit, query, response value.**

API

Application Program Interface. The set of client interface routines your application uses to communicate with the Sentinel system driver, which in turn communicates with the hardware key. *See also* **driver.**

API Explorer

Allows you to experiment with API function calls on various cells in the key before you add them to your source code. It is also a good way to familiarize yourself with the available functions and their uses prior to designing your strategy.

application protection

An algorithm with an associated activation type as determined by the options you choose to include in your strategy. Application protection can be either *integrated* or *automatic*. The protection type determines when and where software locks are implemented. *See also* **automatic protection, integrated protection, software lock, activation type.**

automatic protection

Also known as *shelled* protection. The fastest and easiest method of protecting your applications with SentinelSuperPro.

Instead of adding software locks to your source code, a protective “shell” is automatically added to your application’s executable file, so that the software lock is called before the application starts—if the hardware key is not present, the user sees an error message and the application does not run. Automatic protection also gives you more control over demo options such as expiration dates, counters and time/date limits. *See also* **application protection, shell, software lock.**

C

cell	A memory location on the hardware key that holds 16-bit values. Elements occupy one or more cells on the key.
cell type	A code assigned to each cell that defines (logically) how you want to use the cell. The cell type classifies the type of data stored in the cell, which in turn affects how the cell can be used. Each cell type is identified by a two-letter abbreviation; for example, CW identifies a counter word.
cell value	The 16-bit value contained in each cell. The cell value is also known as a <i>word</i> .
Client Activator	An automated license installation utility that is used to create a product-specific activation script for your protected application. The Client Activator is Rainbow Technologies' recommended means of field activation for SentinelSuperPro protected applications, due to its user-friendly interface. The Client Activator also allows your customers to easily and quickly activate your product via a Web site, if you desire.
command	Function calls that describe what will be done to a key in the field. For example, the Decrement Counter command locates the counter cell on the key and decrements it by the value you specify. <i>See also</i> API .
counter	A cell used to count down from a pre-programmed value. The value in a counter is decremented each time your application sends the RNBOsproDecrement() API function. A counter has an access code of 2. Usually, counters are used to control the number of times a demo application is executed. If desired, a counter can be associated with an algorithm; when the counter reaches zero, the algorithm is deactivated automatically. <i>See also</i> access code, demo, algorithm .

D

- data word** A cell in a SentinelSuperPro key that is used to store information. A data word can store data such as customer information, serial numbers, passwords, and check digits. You code your application to read the word and then evaluate and act upon the stored value.
- Your application can use the stored value to verify the key is still attached, or to control program flow or operation. A data word has an access code of 0 (read/write) or 1 (locked/read-only). *See also* **access code, locked word**.
- decryption** The process of deciphering data that was previously encrypted. Decryption requires a secret key or password. *See also* **encryption**.
- 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. *See also* **counter**.
- Design Stage** The Design stage has two sections: Element List View and Element Layout View. Use the Element Definition Wizard, accessible via Element List View, to define cell types and cell values. Element Layout View allows you to view and modify the location of algorithm, counter and data word cells on the hardware key.
- developer ID** A unique identification code assigned to you by Rainbow Technologies. You must use your developer ID to program your keys. You must also use it in your protected application to establish a connection with a key.

- distributor** Someone outside of your organization who will be responsible for selling and activating your application. For example, distributors could be resellers or fulfillment centers. Distributors must receive a distributor key in order to activate an application using the distributed activation type. *See also* **distributor key, distributed activation type.**
- distributor key** A key given to your sales distributors, allowing them to perform activation and update functions on product keys provided to end-users when they sell your protected application. A counter decrements each time the distributor activates or updates an application. This allows you to keep track of applications activated by your distributor. *See also* **counter, distributed activation type.**
- distributed activation type** Method of product activation provided by SentinelSuperPro where the application is inactive until activated by an activation password. The activation password is different for every key; it is derived from the key's serial number, product information, an encryption engine, and an algorithm located on a distributor key. An application using the distributed activation type will be activated by your distributors using a distributor key. *See also* **activation password, distributor key, activation type.**
- driver** A piece of software that enables the computer to communicate with a peripheral device (the SentinelSuperPro hardware key).
- dual mode** An access mode used when you want your application to use either a local key or a network key. This is the default mode for all SentinelSuperPro-protected applications. When in dual mode, an application will send broadcast messages to the network to locate an appropriate server. *See also* **network mode, access modes, stand-alone mode.**

E

- element** An item in your protection strategy such as an algorithm, counter, data word or application protection.
- encryption** The scrambling of data to prevent unauthorized access. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. *See also* **decryption**.
- encryption seed** A string of bits used to as an input to an encryption function or algorithm. The larger the seed (the more bits in the seed), the greater the number of potential patterns that can be created, thus making it harder to break the code and decrypt the contents.

F

- field activation** A secure method of remotely updating a SentinelSuperPro hardware key's memory after the key is sent to your user.
- Field activation allows you to increase demo limits, upgrade demo applications to fully licensed versions, and provide access to additional modules or features, without having to ship a new key to the customer or visit the customer's site.
- field exchange** Enables you to ship your application in an unusable state, and provide a means for legitimate users to activate it. The activation process is protected by encryption algorithms and passwords pre-programmed into the key. This same process also allows you to support field upgrades and control feature access. *See also* **algorithm, field activation, activation password, active/inactive bit**.

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. *See also* **hardware key, license, sublicense.**
- hardware key** The heart of SentinelSuperPro protection. The key controls and verifies access to your protected applications, assuring that only authorized users can run them
- hexadecimal** A base-16 number system. That is, a numbering system containing 16 sequential numbers as base units (including 0) before adding a new position for the next number. The hexadecimal numbers are 0-9 and then the letters A-F.
- When showing the contents of computer storage, one hexadecimal digit can represent the arrangement of four binary digits. Two hexadecimal digits can represent eight binary digits, or a byte.
- hidden word** A cell that cannot be read by your application. Most hidden words are algorithms and activation passwords. Your write password and overwrite passwords are also hidden words. A hidden word has an access code of 3. *See also* **access code, algorithm, activation password, write password, overwrite password.**

I

Implementation Stage

This stage allows you to add a shell to an application's executable file, or view the pseudocode protection plan generated during prototyping,

This stage also allows you to define the actions that can be taken through field activation, and is used to create license codes for distribution to customers who have purchased upgrades in the field.

inactive application

An application that will not run until it is activated.

integrated protection

A form of application protection where software locks (API function calls) are added directly to your source code. It is used to create a custom protection strategy, with control over the amount and location of software locks. *See also* **software lock, API, application protection.**

L

license

A license allows the user 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 SentinelSuperPro based on the locking code provided by the customer and the actions you select. When the customer enters the license code in the Client Activator or Field Exchange Utility, a script is automatically run that performs the selected actions on the key.

License codes are unique to the key the locking code was generated from. *See also* **action, command, field exchange, locking code.**

locked word

A data word that contains a value that can be read but not changed by your application unless the overwrite passwords are used. A locked data word has an access code of 1. *See also* **data word, access code, overwrite passwords.**

locking code

A code that includes information about how a key is currently programmed, including the key's serial number and developer ID. You must have a customer-generated locking code to create a license code. Locking codes are unique for each key. *See also* **action, command, field exchange, license code.**

M

Make Keys Stage

The Make Keys stage allows you to program keys prior to distribution. Hardware keys programmed with your protection strategy, as defined in the Design stage, must be distributed with each copy of your software.

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 you want *only* a network key to be used. 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. *See also* **access modes, dual mode, stand-alone mode**.

O

Overview Stage Sections in this stage introduce you to SentinelSuperPro concepts. This stage also features the API Explorer, where you can test API function calls, view the key's cell layout, and send queries to the key to obtain return values.

overwrite passwords A set of passwords you must have in order to set or change the value or access code of any cell other than a data word or a cell that is undefined.

Your overwrite passwords are provided to you by Rainbow Technologies. Keep them secure; they have the power to reprogram all unrestricted cells in your key. *See also* **write password**.

P

product key

See **hardware key**.

project

A project is stored in a SentinelSuperPro file. The project contains all the data used to create your protection strategy—elements, passwords, your developer ID, algorithm values, counters, data words, field activation commands, etc.

Your project is the template that will be used to program the keys protecting your application.

Project Stage

This stage provides setup and configuration information. Create or open projects and enter your developer ID and passwords in this stage.

Prototype Stage

In this stage, you program the cells in the hardware key with the values defined in the Design stage, generating pseudocode for use in adding API functions to your source code. *This stage is a required stage.*

pseudocode

Outlines the API functions you need to add to your application (if you are using integrated protection), as well as additional information about your protection strategy.

Q

query

The process by which an application verifies that the hardware key is still attached or has not been tampered with. This is done by sending query data to be scrambled using a specific algorithm stored in the key. *See also **algorithm, query data**.*

query data The value an application sends in a query to the hardware key. The key scrambles the string according to its internal logic and the bit pattern defined in a specified algorithm. It then returns a response to the application. *See also* **response string, algorithm, query.**

R

response string The scrambled result derived when the hardware key processes query data according to the bit pattern contained in an algorithm. The hardware key returns the response string to the application. The application then uses the response to determine whether the user is authorized to run the application. *See also* **query data, algorithm.**

S

server The SentinelSuperPro server manages licensing and security for the protected application. The server is the link between the client running your application and the hardware key, located on the network, that responds to the API functions used in your protection strategy.

shell A protective layer wrapped around your application's executable file when you use automatic protection. This layer is encrypted, making it more difficult for a hacker to gain access to your application's code.

All software locks and communication with the hardware key (such as checking and verification) are handled by the shell. An application protected with a shell can be run only if the user has the correct hardware key. *See also* **automatic protection, software lock.**

software lock

A decision point in an application. The purpose of a software lock is to verify the presence of the correct hardware key.

For example, an application might send query data to the hardware key, and require a specific response in order to continue execution. Other software locks may simply read the value in a cell and compare it to the value known to be programmed in that cell. *See also* **query data**.

stand-alone mode

An access mode used for applications where you want *only* a local key to be used. 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. *See also* **network mode, dual mode, access modes**.

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. Stand-alone keys have a hard limit of 0, meaning the key can be used only by one user at a time. These keys can also be connected to servers, but provide only a single license at any one time. *See also* **network key, hard limit, license**.

sublicense

A sublicense is a license limit you define that is less than or equal to the hard limit programmed into the key. Sublicenses allow you 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 your protected application(s). *See also* **hard limit, license**.

static activation type

Method of product activation provided by SentinelSuperPro where the application is inactive until activated with an activation password, unless it is a demo or metered application. The password is the same for every key used with the protected application. *See also* **activation password, demo**.

T

trusted activation type

Method of product activation provided by SentinelSuperPro where the application is inactive until activated by an activation password, unless it is a demo or metered application. The activation password is different for every key; it is derived from the key's serial number, product information and an encryption engine. *See also* **activation password, demo, activation type**.

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.

W

word

See **cell**.

write password

A password you must have in order to set or change the value or access code of a data word or a cell that is not yet defined. This password also allows you to decrement counters. Your write password is provided by Rainbow Technologies. *See also* **access code, data word, counter**.

Appendix A – Glossary