



December 2005



<b>The Big Picture</b> .....	3
<b>System Requirements</b> .....	5
<b>Installation</b> .....	6
<b>Simple Installation</b> .....	6
<b>Setting Up an Unattended Installation</b> .....	7
<b>Understanding CompuGuard CornerStone</b> .....	8
<b>GUI Access</b> .....	8
<b>Security</b> .....	9
<b>"Remember Password" Option</b> .....	9
<b>Registration</b> .....	11
<b>Evaluation Registration</b> .....	11
<b>Registering Via the CompuGuard Control Center</b> .....	11
<b>Registering Via the Centurion Web</b> .....	12
<b>Protection Mode</b> .....	14
<b>Enabling and Disabling Protection</b> .....	14
<b>Disabling Protection</b> .....	15
<b>Enabling Protection</b> .....	15
<b>Oops!</b> .....	15
<b>USB Blocking</b> .....	17
<b>Storage Configuration</b> .....	17
<b>Temporary Storage</b> .....	18
<b>Configuring the Temporary Storage Size</b> .....	19
<b>Persistent Storage</b> .....	20
<b>Creating Persistent Storage</b> .....	20
<b>Resizing Persistent Storage</b> .....	20
<b>Unmounting the Drive</b> .....	21
<b>Mounting the Drive</b> .....	21
<b>Deleting Persistent Storage</b> .....	21
<b>Remote Management</b> .....	22
<b>Retrieve Updates</b> .....	23
<b>Update Source</b> .....	23
<b>Automatic Updates</b> .....	24
<b>Remote Management Server Configuration</b> .....	24
<b>Miscellaneous Configuration</b> .....	26
<b>Oops! Operations</b> .....	26
<b>Stealth Mode</b> .....	27
<b>Manage Passwords</b> .....	27
<b>Command Line Utility</b> .....	28
<b>Saving "My Documents", Emails, and Internet Favorites</b> .....	29
<b>Technical Support</b> .....	33
<b>License Agreement</b> .....	34

# **The Big Picture**

We at Centurion Technologies, Inc. have taken the same industry leading technology used in our previous hard drive protection solutions and added remarkable functionality. CompuGuard Cornerstone provides systems administrators the ability to do more than just protect their hard drives' configuration. Along with the ability to protect your hard drive, some key features of CompuGuard Cornerstone include:

- The ability to create an additional drive to be used for permanent storage of data.
- USB blocking.
- Able to be remotely managed using the CompuGuard Control Center (CCC).
- The ability to change the current protection status without rebooting.
- Retrieve updates automatically.
- The option to run in "Stealth Mode".
- An easy-to-use GUI.

## **How does CompuGuard Cornerstone Work?**

CompuGuard Cornerstone protects your system by write protecting the hard drive at the physical sector level, similar to the way that you write protect floppy disks by setting the write protect tab.

When an application needs to write to the hard drive, CompuGuard Cornerstone automatically redirects file writes to a separate non-write protected area on the hard drive. All attempted changes to the hard drive are recorded in the storage area. Changed data is read from this specific storage area, instead of the hard drive, appearing as if it had been changed on the hard drive. This method allows full protection of your computer files while still offering maximum access to your system. The next time the system is rebooted, all changes are discarded.

In addition to explicitly protected partitions, CompuGuard Cornerstone also protects any non-file system areas (such as the partition map) on any disk drive that contains protected partitions. CompuGuard Cornerstone will also refuse a request to do a low-level format on any disk drive that contains protected volumes.

**Note:** CompuGuard Cornerstone does NOT protect your BIOS settings. In order to protect your CMOS BIOS settings, you will need to set a supervisor password. Without setting a supervisor password your BIOS settings will be vulnerable to configuration changes, even while your system is protected.

## **Who would benefit from using CompuGuard Cornerstone?**

Anyone maintaining single or multiple computer systems running Windows 2000 and/or XP.

### **The Problem:**

You are a lab administrator at a university and are in charge of maintaining a lab of 30 machines. Throughout the course of a day, hundreds of students use your lab for multiple reasons--to check their email, write papers, surf the internet, use software to complete assignments, etc. As an administrator one of your top priorities is to maintain the integrity of each machine. Having each machine running smoothly is absolutely critical to the success of your lab. However, numerous variables in your environment--student traffic,

internet viruses, adware and spyware, users changing system settings, users deleting/saving data, etc.--can make the attainment of this one goal extremely daunting.

As with any public access computer lab, restoring each machine to its desired configuration can take a great deal of time. The time and energy you and your staff devote towards simple maintenance is not only overwhelming, but unnecessary.

## The Solution:

Enter CompuGuard Cornerstone!

You setup your machines with your desired configuration--software applications, desktop icons and background, internet home page, etc. Once you have everything the way you want it, you install CompuGuard Cornerstone and enable protection on all your machines. Now you let your users loose in the lab. The difference now being the confidence you have that at the end of the day all you need to do is reboot your machine and...whala! Everything is back to the way it began when you first set your machines up.

Now that you are protected with CompuGuard Cornerstone, users can download viruses, accidentally install adware and spyware, change desktop backgrounds, delete important folders, edit the registry, and even alter a machine to the point of crashing. The beauty of it all--it no longer matters. You simply reboot your machines and everything goes back to normal...everything!

## Why use CompuGuard Cornerstone?

- Takes the worry out of maintenance and security issues.
- Dramatically reduces time put towards computer maintenance.
- Offers consistent system configurations.
- Enables an administrator to provide unrestricted access to a user.
- Enhances virus protection.

CompuGuard Cornerstone is designed based on a unique patented technology that has protected libraries, universities, business organizations, and school labs throughout the world. CompuGuard Cornerstone (along with Centurion's other products), is the only hard drive and configuration protection software solution using "**Instant Restore**" technology, ensuring a higher level of security and stability for Windows 2000 and XP systems.

Users can **manipulate the desktop, install software, change settings, and download potentially harmful files** from the Internet! A simple reboot of the computer restores it back to the administrator's pre-defined pristine configuration. CompuGuard Cornerstone simply wipes the session changes away... leaving the computer like new.

# **System Requirements**

This release supports Windows 2000/XP. The installer automatically chooses the correct version for the system in which CompuGuard Cornerstone is being installed.

## **Additional Requirements:**

- Recommended hardware requirements for the Operating System.
- At least 500 MB of available disk space.

## **Optional:**

- If using CompuGuard Control Center, TCP/IP must be installed.
- Windows XP-SP2, Firewall must be disabled or exceptions written for program and Client/Management Communication

# **Installation**

Note: CompuGuard Cornerstone cannot be installed on a machine that has DriveShield or Centurion Guard installed on it. If you have DriveShield or Centurion Guard installed on your machine, please uninstall it prior to installing CompuGuard Cornerstone.

Please be aware that CompuGuard Cornerstone will NOT remove viruses or other malicious code from your system. Do not install CompuGuard Cornerstone on a system that already has problems.

## **Simple Installation**

Begin the CompuGuard Cornerstone software installation by setting your system's configuration to the default conditions you wish to use. This includes any software applications that will be used on the system.

- 1)** Insert the Installation disk into the CD-ROM. If Auto-Play is enabled, the setup process should begin. If not, open the CD and click "*CTILaunch.exe*" to begin. If you are installing from the web download, run "*Cornerstone.<build number>.exe*".
- 2)** When the installation Wizard begins, click "Next".
- 3)** After reading the license agreement, click "I accept the terms of the license agreement" and then click "Next".
- 4)** You will be given seven configuration options to choose from. By default, Cornerstone chooses to configure "Protect All Partitions", "Configure Remote Management (CCC)", "Configure Persistent Storage", and "Install Help Files".
- 5)** After clicking the "Next" button, you will be prompted to enter a password. This password will be used anytime you change CompuGuard Cornerstone's configuration settings. Verify your password by typing it again in the second text field. Click the "Next" button when finished.

Note: When setting up multiple systems with CompuGuard Cornerstone, it is recommended that you use the same password for each system.

- 6)** Setup is now ready for installation. Click the "Install" button to begin installation.
- 7)** If you chose to configure for remote management, you will need to specify the IP address and port number of the machine running the CompuGuard Control Center. By default, both the CCC and Cornerstone will have 25555 as their configured port number.
- 8)** If you chose to configure persistent storage, you will need to specify a drive letter and configure the size for the persistent storage area.
- 9)** The installation Wizard requires you to restart your system to complete the installation process. Choose "Yes, I want to restart my computer now".

## Setting Up an Unattended Installation

Cornerstone does allow for setting up unattended installs. Specifically the installer program, InstallShield, provides the infrastructure for recording "answer files" and running silent installations using a given answer file.

This functionality incorporates command line functions which can be implemented when using remote management tools such as Altiris and Zenworks. Any desktop management solution that provides the ability to run scripts and/or command line functions can be used to remotely run our unattended installation feature.

### Step by Step Instructions:

#### **I. Create an answer file:**

**1)** On a machine that does not have Cornerstone installed, run the following from the command line:

```
"Cornerstone.exe -r -f1<path_to_answer_file>"
```

It is important not to have a space between the -f1 flag and the path to the file name.

**Example:** If you want the answer file to be called *answer.iss* and be saved under a directory named 'test'--the command will be:

```
'Cornerstone.exe -r -f1c:\test\answer.iss'
```

**2)** Go through the installation wizard--all answers to the wizard will automatically be recorded to the answer file.

#### **II. Distribute the installation package and the answer file to the clients.**

#### **III. Silently run an unattended setup on each of the clients.**

**1)** On each client, run the following command in order to start the silent installation:

```
"Cornerstone.exe -s -f1<path_to_answer_file> -f2<path_to_log_file>"
```

It is important NOT to have spaces after the -f1 and -f2 flags.

**Example:** If the answer file is in a directory named 'c:\test' and the answer file is called *answer.iss* the command line will be:

```
'Cornerstone.exe -s -f1c:\test\answer.iss -f2c:\test\answer.log'
```

This will run the installation silently using the provided answer file.

# Understanding CompuGuard CornerStone

To better understand CompuGuard CornerStone and all its functionality, it is best to begin by familiarizing yourself with the main components and windows used to manage your CompuGuard CornerStone software.

CompuGuard CornerStone has a GUI Component with five different sections that you will work with to manage your software: —“Protection Mode”, “Storage Configuration”, “Remote Management”, “Misc. Configuration”, and “Registration”. Each of these components helps manage CompuGuard Cornerstone’s powerful capabilities and aide in providing an easy-to-use means of working with the software.

**Note:** The “Registration” Section will disappear once an order number has been entered or a license is granted from the CompuGuard Control Center.

## GUI Access

Once the product has been installed, you will need to access the GUI to make any adjustments or changes to the configuration of CompuGuard CornerStone. Accessing the GUI is a two step process, depending on the protection Mode. When enabled, you must use the Hotkey to initiate the System Tray Icon (in Stealth Mode) and then double click on the Green Shield; when disabled, double click on the Red Shield. This brings up the CompuGuard CornerStone GUI Interface with access to all the configuration settings.



## Security

Any changes made to CompuGuard Cornerstone's configuration settings will require an administrator to enter their password. This is the password you create during the installation of Cornerstone. Each time a setting is changed, you will be prompted to enter your password. If you have multiple changes to make to Cornerstone's configuration settings or do not want to retype your password more than one time during a session, you can check the ["Remember Password" option](#).



### **Why does Cornerstone require me to enter a password when I change its settings?**

The reason Cornerstone requires a user to enter a password when making changes to its settings is simple...**SECURITY**. Requiring a password verifies that an authorized user, and not just anyone, is changing Cornerstone's configuration.

### **"Remember Password" Option**

If you have multiple changes to make to Cornerstone's configuration settings or do not want to retype your password more than one time during a session, you can check the "Remember Password" option. As a result, you will only be required to enter your password the first time a change is made. If the "Remember Password" option is not checked, you will be required to enter your password after each change.

**NOTE:** By default the "Remember Password" option is not enabled.

### **How does an administrator benefit from all this?**

- Able to maintain a high level of security.
- Quickly and efficiently change configuration settings.

Due to the nature and intended use of this software, it is imperative that security standards are high. At the same time, having to enter the same password over and over when making multiple changes can be time consuming and unnecessary. Requiring a password **and** having the ability to remember the password during a session provides a balance between these two concerns.

## If I choose the "Remember Password" option, will the next user be able to change Cornerstone's settings?

**NO.** Each time Cornerstone is opened a password is required at least the first time a setting is changed.

Note: The "Remember Password" option will only apply to the current session of Cornerstone. Meaning, when the "Done" button is clicked or the application is closed, the session is over and the "Remember Password" function is reset to its default. The next time Cornerstone is opened, the user will be required to enter a password to change any settings.

### Example:

An administrator immediately needs to make a few configuration changes to Cornerstone's settings in her computer lab. She is not using the CompuGuard Control Center to manage her clients, so she must change each machine's settings manually. To save time, she decides to check the "Remember Password" box. Now she's only required to enter her password one time at each machine.

Since the lab is still open and quite full, a user is highly likely to sit down at a machine directly after she finishes configuring it. However, she closed the Cornerstone application so now any user after her will not be able to modify Cornerstone's settings without retyping a password.

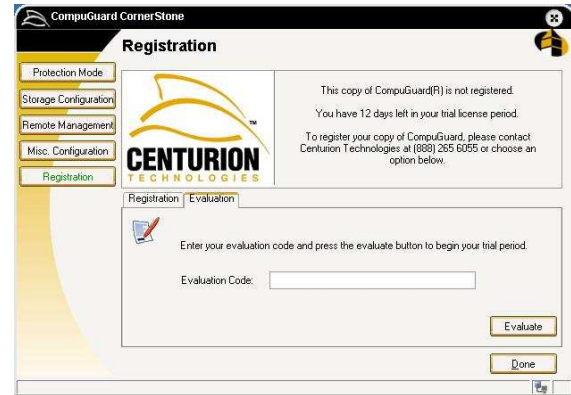
*For more on managing passwords, go to the [Manage Passwords](#) section.*

# Registration

CompuGuard CornerStone is provided with a fully functional evaluation period. Evaluation codes can be provided by your Sales Representative or Technical Support. If you registered as an evaluator, you should have received the appropriate codes when you received your registration confirmation email. This code allows you to use CompuGuard CornerStone and all its functionality for a period of time before you are required to register the software with an order number. You may register CompuGuard CornerStone at any time during the evaluation period. The Evaluation period begins at the time you first download the software.

## Evaluation Registration

- 1) Go to the "Evaluation" tab in the Registration section.
- 2) Enter your evaluation code.
- 3) Click the "Evaluate" button.

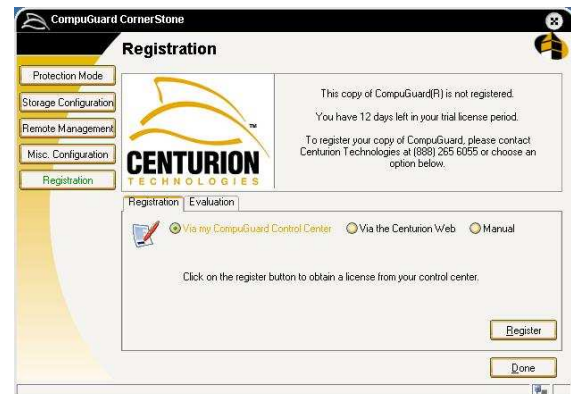


## Registering Via the CompuGuard Control Center

This option is for users who are remotely managing Cornerstone with the CompuGuard Control Center (CCC). From the CCC, you are able to pull your licenses from our licensing servers and hold them in your CCC to be distributed to any connected client machines. You can perform the registration either from the client or from the CCC.

### How do I register thru my CompuGuard Control Center?

- 1) You must have licenses available in your CCC. For more information on adding licenses to your CCC, see the "Help" section in the CCC application.
- 2) Choose the "Via my CompuGuard Control Center" option in the Registration Options section.
- 3) Click the "Register" button.



**Note:** If you are running the CCC, or are planning on running the CCC, you are still able to register with one of the other two options.

## **Registering Via the Centurion Web**

When registering via the Centurion Web, your client machine is retrieving a license by connecting directly to Centurion Technologies' licensing servers. You will need an order number and an open internet connection with all inbound and outbound traffic being allowed on port 8080.

### **How do I register thru the Centurion Web?**

- 1)** Choose the "Via the Centurion Web" option in the Registration Options section.
- 2)** Enter your order number in the text field box. You can manually enter your order number or enter the number from a file. Your order number is provided when you purchase licenses.
- 3)** Click the "Register" button.



### **Why use the "Fill From File" and "Save To File" functions?**

Often times you will have multiple machines to register at one time. In this scenario, it can become arduous to repeatedly enter your order number manually. An alternative to this is to enter your order number one time, save it to a file (on a disk), take that file to each machine and use that instead of manually entering the order number each time. This is also a great way to keep track of your order number(s).

### **Steps for using a file with your order number:**

- 1)** At the first machine, manually enter your order number.
- 2)** Insert a disk into the floppy drive and click the "Save to File" button.
- 3)** Save the order number to a file on the floppy disk.
- 4)** Register the machine.
- 5)** On the rest of your machines, insert the floppy disk and choose the "Via the Centurion Web" option from the Registration Options section.
- 6)** Click the "Fill from File" button.
- 7)** Choose the file from the floppy drive (A:\). This will fill the text field box with the order number contained in the file.
- 8)** Click the "Register" button.

## **Registering Manually**

If you need to register a machine that does not have internet access, or for some reason is unable to register via the Centurion Web, you will need to manually register the Cornerstone software. As with registering via the Centurion Web, you are able to use a file to fill the text field boxes in order to expedite the process.

### **How do I register Cornerstone manually?**

In the text field boxes, you will need to enter your email address, order number, and activation number. Once this information is entered correctly in the text field boxes, click the "Register" button and the Cornerstone software will then become registered.

### **Why would I want to, and how do I, use the "Fill From File" and "Save To File" functions when manually registering?**

Often times you will have multiple machines to register at one time. In this scenario, it can become arduous to repeatedly enter your information manually. An alternative to this is to enter your information one time, save it to a file (on a disk), take that file to each machine and use that instead of manually entering the information each time. This is also a great way to keep track of your registration information.

### **Steps for using a file with your registration information:**

- 1)** At the first machine, manually enter your email address, order number, and activation number.
- 2)** Insert a disk into the floppy drive and click the "Save to File" button.
- 3)** Save the information to a file on the floppy disk.
- 4)** Register the machine.
- 5)** On the rest of your machines, insert the floppy disk and choose the "Manual" option from the Registration Options section.
- 6)** Click the "Fill from File" button.
- 7)** Choose the file from the floppy drive (A:\). This will fill the text field box with the information contained in the file.
- 8)** Click the "Register" button.

## **Protection Mode**

Within the "Protection Mode" GUI an administrator is able to define and apply the desired protection status to a system's drive and USB ports. Each option has a red or green circle signifying the option's protection status. Red indicates protection is disabled. Green indicates protection is enabled.

### **What does it mean when my system is protected by Cornerstone?**

Cornerstone write-protects the hard drive and records all changes to a temporary storage area. The design of the application manages the computer to behave as if all changes are permanent providing a full user experience. However, upon reboot, all changes (actually written to the temporary storage space) are wiped free from the computer instantly restoring your system to its established configuration.

This allows an administrator to set up a system to their desired configuration and not have to worry about a user altering a single system setting. Whether a user downloads viruses, Adware, Spyware, malicious scripts, changes local settings, deletes files, moves folders, etc. With a simple reboot, the protected machine goes back to its predefined configuration. Instant Restore technology is the nucleus of Cornerstone's powerful features and provides benefit to both an administrator and the user.

### **What are the benefits of protecting my system?**

- All configuration changes made to your computer are temporary.
- Assure an operational computer.
- Enable users to experiment without harm.
- Eliminate most maintenance issues saving significant time & expense.
- Protect from viruses even before antivirus companies are aware a virus exists.
- Enable safe internet surfing from Spyware, Adware, and other malicious scripts.

## **Enabling and Disabling Protection**

The "**Next Boot Protection Mode**" allows a user to define the protection status the next time the system is rebooted. The red or green circle on the left side of the row will reflect the protection status upon rebooting your system. This does not necessarily reflect the current protection status.

When a CompuGuard Cornerstone's protection status is "Enabled", any changes a user makes to the system will be erased upon reboot. If changes were made to a system's configuration while protection is enabled and an administrator wishes to make these changes permanent, they may invoke the [Oops!](#) function to override the protection status.

## Why would an administrator change protection status?

### **Disabling Protection**

The main reason to disable protection on a machine is if you need to make a permanent change to the system's configuration. Whether you want to install new software, create additional folders, install Windows updates, etc. protection must be disabled for any change to be permanent. Even when logged in as an administrator, you must disable protection before making any changes to your system's configuration.

#### **To disable protection:**

- 1) Enter your hotkey to display the green shield in your Taskbar. The default hotkey is Ctrl + Alt +F10. If you are not running in Stealth Mode, you will not need to enter a hotkey as the green shield will already be visible.
- 1) Click the "Unprotect" button. Upon exiting the CompuGuard Cornerstone window, you will be prompted with the following message to reboot your machine.
- 2) Click "Yes" to reboot your computer. If you choose not to reboot, you will not be unprotected until you reboot your computer manually.

### **Enabling Protection**

When your system is set to its desired configuration, you must enable protection in order for CompuGuard Cornerstone to protect your machine.

#### **To enable protection:**

- 1) Click the "Protect" button. Upon exiting the CompuGuard Cornerstone window, you will be prompted with the following message to reboot your machine.
- 2) Click "Yes" to reboot your computer. If you choose not to reboot, you will not be protected until you reboot your computer manually.

## **Oops!**

The Oops! command allows an administrator to change the protection status, since the last boot. When an administrator invokes the Oops! command, the current protection status is changed without requiring a reboot. Without Oops!, the only way to change the current protection status is to click the "Protect" button and reboot your machine. The main reason for using the Oops! function is if the current protection status was set to an undesired state and/or the protection status needs to be changed immediately.

**Note:** It is strongly recommended that you carefully read ALL of the below information to fully understand the Oops! command.

### **How does Oops! work?**

**Note:** In order to use the Oops! command you must have "Oops! operations" enabled in the [Misc. Configuration](#) section. It is also strongly recommended that you read the "[Oops! Operations](#)" information in the Misc. Configuration section.

When the "Oops! operations" setting is disabled, the only time Cornerstone records information to its temporary storage area is when the current protection status is set to "enabled". When the "Oops! operations" setting is disabled and the current protection status is set to "disabled" as well, Cornerstone does not write to, nor does it need, the temporary storage area. For more information about temporary storage, see "[Temporary Storage](#)" in the Storage Configuration section.

When an administrator allows for Oops! operations to be available, Cornerstone is recording information to your temporary storage area at all times, even if protection is currently disabled. By allowing the Oops! command to be used, Cornerstone is now recording any and all configuration changes a user makes. Regardless of the current protection status, these changes are being written to the temporary storage area. When Oops! operations are enabled Cornerstone is then able to *reverse* all changes that were made while protection was disabled and also able to *apply* all changes that were made while protection was enabled.

### **How is using Oops! different than the regular method of changing protection?**

When changing the protection status of a system via the "regular" method--Clicking the "Protect"/"Unprotect" buttons--you must reboot your machine for the change to take effect. The Oops! button allows you to change the protection status immediately.

**Note:** When you click the Oops! button, the protection status change is applied to the beginning of the last time your machine was booted, until the next time you change the protection status. For this example only, a session can be defined as the period of time from one boot to the next. Keeping that in mind, the Oops! function will change the protection status for that entire session.

### **Why would I want to use the Oops! function?**

There are many different reasons why and when an administrator may choose to use the Oops! function. Below are a couple examples.

#### **Example 1:**

A user boots the system in a protected state. While the system is protected, the user makes changes to the system that need to be permanent. Now, with the Oops! feature, an administrator clicks the Oops! button and the system changes to an unprotected state and the user's changes become permanent. The system acts as if it were in that state since the last time it booted.

#### **Example 2:**

A user boots the system in an unprotected state. While the system is unprotected, the user downloads a virus and makes unwanted changes to the system's configuration. An administrator clicks the Oops! button and the system acts as if it were protected the entire time the user was operating the system.

## **USB Blocking**

With USB Blocking, an administrator has the ability to permit and prevent access to all USB ports on a system. This prevents any reading from and writing to USB storage devices. Additionally, an administrator can invoke USB blocking without having to reboot their system.

A red circle indicates all USB ports are currently unblocked. A green circle indicates all USB ports are currently blocked.

### **How can I benefit from USB Blocking?**

Anytime an administrator needs to deny a user the ability to read from or write to a USB storage device all they need to do is click the "Block" button in the USB Blocking section. When a teacher needs to administer a test to their students often times they do not want the student to have the ability to use external data or copy data to a storage device. In this situation, USB blocking can add extra protection to facilitate such a need. USB blocking also prevents viruses from being downloaded to a system from an external USB storage device.

**NOTE:** USB blocking will only block reading from and writing to storage devices. It will not interfere with other technologies that may be utilizing a system's USB ports.

## **Storage Configuration**

Within the Storage Configuration functionality an administrator has the ability to:

- Define the "Temporary Storage" size on an existing drive.
- Create an additional drive for "Persistent Storage" and define its size.
- Easily keep track of drive specifications.

### **How can I benefit from the functionality provided in the Storage Configuration window?**

The storage configuration options benefit an administrator by allowing them to define and create the necessary structural components used by CompuGuard Cornerstone. At the same time, it provides the needed information regarding your system's current drive(s). The information and functionality provided thru the Storage Configuration window will assist you in setting up Cornerstone's temporary and persistent storage areas.

It is highly recommended that you read the information regarding both [Temporary Storage](#) and [Persistent Storage](#) before modifying any storage configuration settings.

## **Temporary Storage**

CompuGuard Cornerstone will detect your hard drive and any additional partitions or drives on your system. Each drive can then be given a temporary storage area (a temporary storage area is automatically given to the system drive during installation). The temporary storage area is used only on drives you wish to be able to protect. A drive can be left unprotected by using the "stop guarding" option. The temporary storage area is used when Cornerstone's protection is enabled and/or when Oops! operations are enabled. Cornerstone uses this area for reading and writing data to and from the drive. The temporary storage area's size can be increased, decreased, or left at its default size. When determining the size of the temporary storage area, an administrator should take into account the manner in which the system is currently being used and how it will be used in the future.

### **How exactly does Cornerstone use the temporary storage area?**

The temporary storage area is a file (not accessible to a user) that Cornerstone uses for writing, reading, and tracking the changes a user makes to the system. When a user makes a change to any data on the system, Cornerstone is tracking and writing all the user's changes into the temporary storage area. It is also reading all these changes from the temporary storage area. So in actuality, the system reads and writes the user's changes to and from that location only; never altering the "actual" information on the hard drive. However, to the user it appears as if the changes are actually being saved.

If the current protection status is set to "enabled" at the time of a reboot or shutdown, the information in the storage area is cleared and will not be written to the hard drive.

If the current protection status is disabled and Oops! operations is enabled, Cornerstone will be using the temporary storage area the same way as described above with one important difference--Cornerstone sees that the current protection status is set to "disabled" which means that all changes made to the system during the current session should become permanent. Now, if the system is rebooted or shutdown, the changes in the storage area are written to the hard drive. For more information on using the Oops! command see "[Oops!](#)" in the Protection Mode section.

The only time the temporary storage area is not being used is when both the protection status and Oops! operations are currently set to "disabled". For more information on setting the protection status see the [Protection Mode](#) section.

### **Why would I want to increase the temporary storage size?**

**User's Needs:** If a system is being used to manipulate large files while running memory intensive applications, an administrator would want to increase the storage area based upon their user's needs. This situation often occurs when systems are used primarily for graphics manipulation.

**Oops! operations are enabled:** When the "Oops! operations" setting is set to allow Oops! operations, Cornerstone needs to be writing to the storage area at all times. This increases the chance that the storage area may become full. In most situations, having Oops! operations set to enabled should not require the storage area to be increased. For more

information on enabling and disabling Oops! operations see "[Oops! operations](#)" in the Misc. Configuration section.

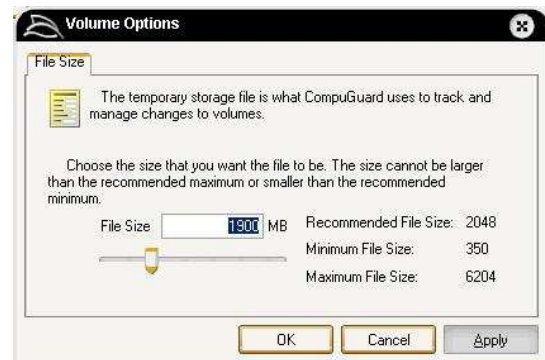
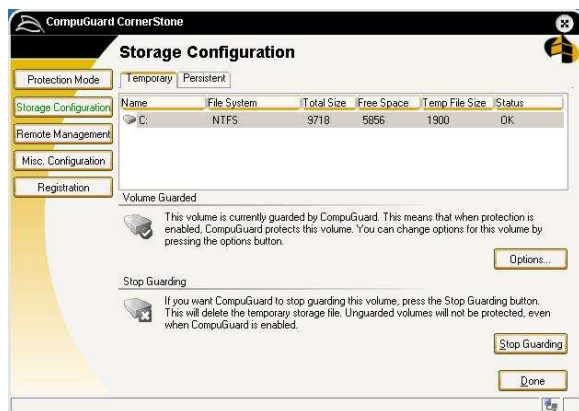
## How will I know if the temporary storage size needs to be increased?

When the temporary storage area becomes full and data is still being written to it, your machine will give "**Delayed Write Failed**" errors. These errors are generated by Windows and can occur when Oops! operations is set to enabled or when Cornerstone's current protection status is set to "enabled".

**NOTE:** The temporary storage size can be altered at any time as long as the current protection status is set to disabled.

## Configuring the Temporary Storage Size

- 1) From the "Temporary" tab, select the drive you wish to configure.
- 2) Click the "Options..." button.
- 3) In the "Volume Options" window, configure the size (in MB) of the temporary storage area.



## Stop Guarding a Drive

**Note:** This cannot be applied to the system drive and protection must be disabled for this option to appear.

- 1) Highlight the drive you wish to leave unprotected.
- 2) Click the "Stop Guarding" button.

**NOTE:** Cornerstone will identify all drives currently detected by Windows. If your system has a dual boot configuration with two or more hard drives, where the hard drive being booted to cannot see the other drive(s), Cornerstone will not be able to detect the other drives. If you have this configuration and want all your drives protected, you will need to install Cornerstone on each drive.

## Persistent Storage

Persistent Storage is an area created by Cornerstone to allow users to permanently save data while protection is enabled. This area is given a name, assigned a drive letter, configured to a size. Data saved on the persistent storage drive will remain on a system even when the machine is rebooted from a protected state.

With the Persistent Storage functionality, an administrator is able to create an additional drive that is preconfigured to always stay unprotected. This will allow users to save their work permanently; even when the system is booted into a protected state.

### Why would you want to create persistent storage?

There are many reasons an administrator may want to create an additional drive for persistent storage, but the most obvious reason is simple...to allow users the ability to save data locally. Without creating a persistent storage area, a user is limited to saving data to a floppy disk, a zip disk, burning to a CD or DVD, saving to other removable storage devices, or uploading files to a remote location. Now, with the persistent storage functionality an administrator is able to protect a system's hard drive while providing a user with the ability to persistently store data locally.

### Creating Persistent Storage

The default setting during installation is to create persistent storage. If the persistent storage drive was deleted or not created during installation, the option to create it will be displayed.

- 1) Click the "Create" button.
- 2) Choose a drive letter and set the size (in MB).
- 2) You must restart your computer to begin using the persistent storage drive.



### Resizing Persistent Storage

To resize the persistent storage drive, it must be [deleted](#) and [created](#) again. Before deleting the drive, be sure to backup all the information on the drive.

### Why would you want to unmount and mount a drive?

Unmounting a drive is quite useful in environments with multiple types of users, who are using the same machine, and storing data they do not want made available to the next user.

## Example Situation:

You have a computer lab that is used to teach a programming class. Along with the programming class using the lab, it is also open for public use during the weekends. The instructor assigns a machine to each student and needs each student to be able to save data to their respective machines. At the same time, the data being saved are projects and assignments that other users cannot and should not have access to. As a computer lab administrator, it is your responsibility to accommodate this situation.

## Solution:

You have CompuGuard Cornerstone protecting each machine's system partition. For the programming class you create an additional drive that is set up for persistent storage. Once you have configured a drive for persistent storage (i.e. set the storage size, assigned a drive letter, mounted, and formatted the drives), you are now ready to implement a schedule for mounting and unmounting the drive.

When the programming class is in session, each machine has the "programming class" drive mounted. When the weekend comes and when the class is not in session, the drive is unmounted so the public access users do not have access to the students' work.

This solution allows for the class to have their own persistent storage drive, the ability to manipulate data on their drives, restricts unwanted users from accessing the students' work, all while maintaining the integrity and protection of the system partition.

## Unmounting the Drive

When a drive is unmounted it is no longer available to the user. All data stored on the drive will remain on the drive until the drive is deleted.

- 1) Click the "Unmount" button.
- 2) Enter your Cornerstone password.

## Mounting the Drive

When a drive is mounted, the drive and all data stored on the drive become available to the user. A user will have the ability to save, modify, and delete all data on the drive.

- 1) Click the "Mount" button.
- 2) Enter your Cornerstone password.

## Deleting Persistent Storage

- 1) Click the "Delete" button.
- 2) Enter your Cornerstone password.

**NOTE:** When you delete a "Persistent Storage" drive, the drive and all its contents will be permanently erased and no longer accessible.

# Remote Management

With remote management, Cornerstone is able to accept advanced remote management commands from the CompuGuard Control Center (CCC) product. In Cornerstone, the remote management options allow an administrator the ability to define various remote management configuration settings. When running CompuGuard Cornerstone in conjunction with the CompuGuard Control Center you will at least need to configure CompuGuard Cornerstone to the CompuGuard Control Center's IP address and port #.

## What are some of CompuGuard Control Center's capabilities?

CCC provides an administrator with numerous capabilities and endless possibilities. CCC may be purchased separately to control all Centurion Technologies hard drive protection products and offers exclusive features. CompuGuard Control Center provides:

- **Grouping & Filtering**—Multiple clients can be filtered and grouped by specific criteria (i.e., machines on a specific subnet, machines with a specific OS installation, machines with a specific naming substring, etc). You may also manually create your own groups inside the CCC's easy to use GUI by simply creating a folder and copying & pasting a client into it.
- **Broadcast Updates**—Centurion application updates can be broadcast from an administrative server eliminating individual updates.
- **Remote Shutdown & Wake On LAN**—Remote shutdown and "wake" of client machines.
- **Server Integrated Scheduling**—Scheduling of commands to be applied to clients. This allows the ability to integrate all the CCC's commands along with it's filtering capabilities and implement a schedule based upon your needs.

## What are the benefits of remotely managing my CompuGuard clients?

- **Time!**—Not being spent at each client machine.
- **Time!**—How little it takes to set up and configure the perfect self-maintaining environment.
- **Time!**—That can now be spent on other things.

The CCC is without a doubt, the most powerful tool in the CompuGuard product suite. It not only meets every remote management need within the spectrum of hard drive protection...it completely redefines the concept of "Remote Management". CCC, along with having an extremely user friendly GUI, gives you the ability to execute almost every command available (plus some added commands) and apply them to your client machines from a remote location.

CCC also allows you the ability to filter your clients into groups based upon your needs. In addition, you are able to save your chosen groups so that they may be used at any time. This is proves to be especially useful when it is necessary to execute remote commands, at different times, on the same group of client machines. With this in mind, one client can belong to multiple groups and you are able to rotate which groups to display and invoke commands on at any given time.

Now, combine all this with the ability to schedule a time for your chosen commands to be executed upon your specified groups of clients and you have begun to design your own dynamic, almost maintenance-free, server-managed environment.

## **Retrieve Updates**

By clicking the "Update Now" button, an administrator is able to retrieve any available updates to the CompuGuard client. If there are available updates, they will be installed immediately. By clicking the "Update Now" button, CompuGuard Cornerstone will retrieve available updates either from the CompuGuard Control Center or via the Centurion Web. You can decide where CompuGuard Cornerstone looks for updates in the "[Update Source](#)" row of the Remote Management window. You can also choose to have CompuGuard Cornerstone automatically check for updates by [enabling automatic updates](#).

### **Why use the "Update Now" button?**

The "Update Now" button allows a user to retrieve Cornerstones' updates at a specified time. If you are not running the CCC and do not want Cornerstone to update itself automatically, you must use the "Update Now" button. This also gives an administrator some freedom to decide when to retrieve updates. If you are in an environment with limited bandwidth and heavy network traffic during specific times of the day, you might want to disable automatic updates and use the "Update Now" button to update at a time when your network traffic is lower.

## **Update Source**

By choosing either "CompuGuard Control Center" or "Centurion Web", an administrator can specify the location of where Cornerstone will download its updates. The specified location, applies to both automatically and manually updating Cornerstone.

**CompuGuard Control Center:** Connects to, and downloads updates from, the CompuGuard Control Center (CCC). In order to retrieve updates from the CCC, you must have CCC installed on a machine that is able to establish a connection to your Cornerstone client.

**Centurion Web:** Connects to, and downloads updates from, the Centurion Technologies' server. To download updates from the Centurion Technologies' web site your client machine must have a working internet connection and your firewall settings must allow Cornerstone to download data.

**NOTE:** If Cornerstone is being managed with the CCC, it should be configured to check for updates from the CompuGuard Control Center.

### **What are the benefits of obtaining updates from my CCC or from Centurion Technologies' web site?**

- **CCC**—By choosing to receive your from the CCC, you are able to schedule from the CCC when a client downloads its updates.
- **Centurion Web**—Updating from Centurion's website will benefit users who are not running the CCC.

## **Automatic Updates**

### **Enabling Automatic Updates**

By checking the box "Enable Automatic Updates", CompuGuard Cornerstone will periodically check for updates. Cornerstone will retrieve available updates either from the CompuGuard Control Center or via the Centurion Web. Even with "Automatic Updates" enabled, at any time you can manually retrieve updates by clicking the "Update Now" button in the "Retrieve Updates" section. You can decide where CompuGuard Cornerstone looks for updates in the "[Update Source](#)" row of the Remote Management window.

### **Disabling Automatic Updates**

To disable CompuGuard Cornerstone from automatically checking for updates, do not check the box "Enable automatic updates". If you disable the "Automatic Update" function, you will need to check for updates manually.

### **What are the benefits of enabling or disabling automatic updates?**

- **Enabling automatic updates**—Ensures that all the necessary updates will be installed even if you forget to manually update. This also guarantees timely installation of updates and potentially reduces the time Cornerstone will go without being updated.
- **Disabling automatic updates**—Gives an administrator the freedom to decide when to retrieve updates and prevents Cornerstone from updating at an undesired time. This can be useful in an environment with limited bandwidth and heavy network traffic during specific times of the day.

## **Remote Management Server Configuration**

This section allows an administrator to configure the CompuGuard client for remote management by specifying the IP address or computer name of the machine running the CompuGuard Control Center and the port on which the two communicate. In order for a client to be controlled remotely, it is required that CompuGuard Cornerstone be configured to the CompuGuard Control Center's IP address or computer name.

### **Requirements:**

- TCP/IP must be installed.
- You must be able to ping between the machine running CompuGuard Control Center and the CompuGuard Cornerstone client.
- There must be open communication allowed on CompuGuard Control Center's and the CompuGuard Cornerstone's configured port #s.

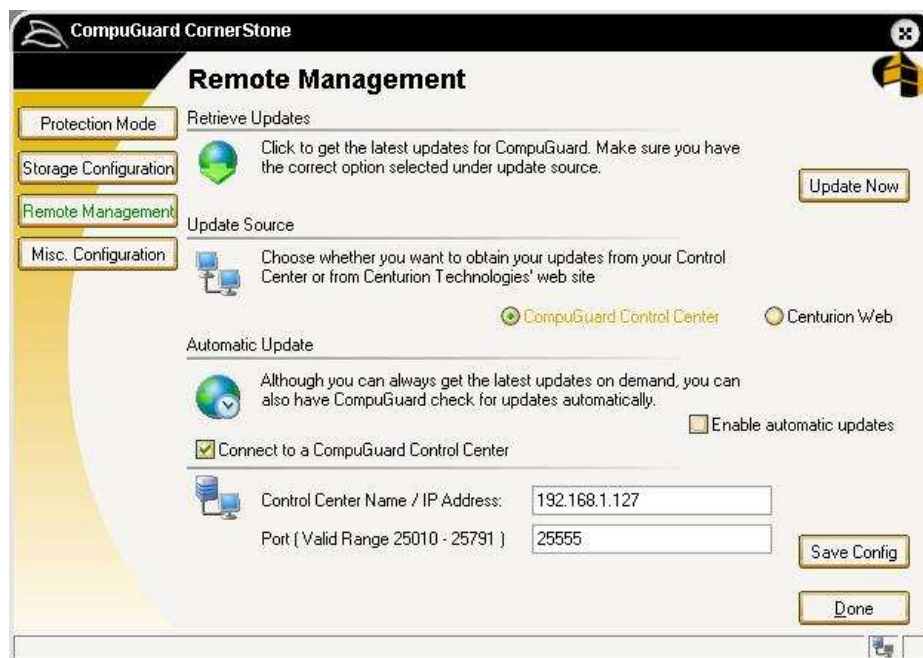
## **Configuring CompuGuard Cornerstone for Remote Management**

**1)** Obtain the IP Address of the machine running CompuGuard Control Center and enter the IP Address in the "IP Address" text field.

**NOTE:** If the machine running the CompuGuard Control Center has a dynamic IP address, choose the "Server Name:" option and enter the computer name in the text field. It is not necessary to use its DNS suffix.

**2)** Enter the port # to be used for communication between the CompuGuard Control Center (CCC) and CompuGuard Cornerstone. The port # should be the same for both the client and the CCC machine.

**3)** When you have finished entering the IP and port information, click the "Save Config" button to save your configuration changes.



## **Miscellaneous Configuration**

This section contains the settings to allow an administrator the ability to allow the Oops! operations, to set CompuGuard Cornerstone to run in Stealth Mode when protection is enabled, and to manage user passwords.

### **Oops! Operations**

This setting provides an administrator the option to enable or disable the use of Oops! operations. When the "Allow Oops! Operations" box is checked, Oops! operations are enabled and the Oops! command can be executed. When the "Allow Oops! Operations" box is not checked, Oops! operations are disabled and the Oops! command may not be used. For more information on the Oops! command, see "[Oops!](#)" in the Protection Mode section.

**NOTE:** After enabling the Oops! operation, you must restart your system. If you have Oops! disabled while your machine is protected, you will NOT be able to use the Oops! operation. You will need to reboot your system in order for the Oops! operation to become accessible. Rebooting your system from a protected state will result in a loss of all data from that protected session.

### **What are the benefits of allowing or disabling Oops! operations?**

#### **Benefits of disabling Oops! operations:**

- Increases your systems processing abilities.
- Allows for a user to utilize a greater amount of the temporary storage area.
- Your system does not need to keep track of as much information.

#### **Benefits of enabling Oops! operations:**

- Provides a higher level of system control by allowing Oops! operations to be executed.
- Gives an administrator the ability to correct potentially harmful mistakes.

### **After enabling the Oops! operation, why is it necessary to reboot my computer?**

In order for Oops! operations to work, your machine must have a temporary storage area set up that tracks all the activity on the machine. This temporary storage area can only be created and made active when your machine boots up.

## Stealth Mode

This option provides an administrator with the ability to enable or disable Stealth Mode. Enabling Stealth Mode will prevent users from seeing the CompuGuard icon while your system is enabled. When Stealth Mode is disabled, the CompuGuard shield is visible in the Taskbar.

If your system is currently protected and you are running in Stealth Mode, at any time you can enter your hotkey combination to display the CompuGuard shield. Once the icon is displayed, double clicking the shield will open the Cornerstone application.

### Why would I want to run in Stealth Mode?

Stealth Mode allows Cornerstone to run without a user being aware of its presence. This provides an added layer of security between the user and your system.

**NOTE:** Although Stealth Mode is a valuable feature, running in Stealth Mode is not an absolute necessity for protection. CompuGuard Cornerstone always requires a password to make any configuration changes to its settings.

## Manage Passwords

This feature allows an administrator the ability to manage up to two additional user passwords. The additional user passwords allow the same user rights as the administrative password. Only the administrative user can add, change, or remove additional passwords.

### Adding Passwords

- 1) Click the "Add" button in the Manage Passwords section.
- 2) Enter the administrative password and the new user password.

### Changing Passwords

- 1) Click the "Change" button in the Manage Passwords section.
- 2) Enter the administrative password, the password to change, and the new user password.

### Removing Passwords

- 1) Click the "Remove" button in the Manage Passwords section.
- 2) Enter the administrative password and the user password to delete.

# Command Line Utility

CompuGuard Cornerstone has a command line utility called *ctcmd.exe*. This command line utility is located in the 'C:\Program Files\Centurion Technologies\CompuGuard Cornerstone\' folder. It provides command line control of Cornerstone by allowing an administrator to have almost all the functionality of the Cornerstone GUI.

## How to Run *ctcmd.exe*:

- 1) You must run *ctcmd.exe* from the Windows command prompt: Open the "Start" menu > choose the "Run..." option > type 'cmd' and press "Enter".
- 2) Change the command prompt focus to 'C:\Program Files\Centurion Technologies\CompuGuard Cornerstone>'.  

```
C:\Program Files\Centurion Technologies\CompuGuard Cornerstone>
```
- 3) Type 'ctcmd -h' to list the available Cornerstone command line switches. This will display the proper syntax for entering commands. The window below is what will be displayed in the command window.
- 4) To display Cornerstone's current configuration, type 'ctcmd status' at the command prompt. The below window is an example of what will be displayed.
- 5) When a valid command is entered, a verification will be displayed between the command and the next prompt. A correct command will be verified with the word "OK." printed below it. The below window is an example of a command being executed properly. The command below is configuring Cornerstone's "USB Blocking" setting to unblock all USB ports (with the password 'aaaaaa').

```

C:\WINDOWS\System32\cmd.exe
C:\Program Files\Centurion Technologies\CompuGuard CornerStone>ctcmd -h
CompuGuard command line utility version 1.0
(www.centuriontech.com)

Usage:
ctcmd <command> <flags>
ctcmd -h for a list of commands
ctcmd <command> -h for specific command syntax

Commands:
status:
ctcmd status

enable:
ctcmd enable -p <password>

disable:
ctcmd disable -p <password>

oops:
ctcmd oops -p <password>
Note: will automatically detect the current protection mode.

usb:
ctcmd usb [ -block | -unblock ] -p <password>

storage:
ctcmd storage [ -create | -delete | -resize ] <driveletter> -s <size in MB> -p <password>

pstorage:
ctcmd pstorage [ -mount | -unmount ] -p <password>

config:
ctcmd config -updatesource [web | ecc] -p <password>
          -autoupdates [on | off] -p <password>
          -allowoops [yes | no] -p <password>
          -stealth [on | off] -p <password>

version:
ctcmd version

C:\Program Files\Centurion Technologies\CompuGuard CornerStone>

```

# Saving "My Documents", Emails, and Internet Favorites

The below instructions give the necessary steps for moving the required files/folders to the persistent storage drive. These steps will prove useful when implementing Cornerstone as a hard drive protection solution for users who need to be able to save data to their "My Documents" folder, emails using Outlook, and/or internet favorites in Internet Explorer.

## Moving "My Documents" to Persistent Storage

Moving the **"My Documents"** folder from the **C:** drive to a different drive and/or renaming the folder to something different is not as straight forward as renaming or moving any other folder on a Windows system but it is not that much more complicated either.

- 1)** The first step is to create the new folder that you want to use in place of **"C:\My Documents"** and place it in the Persistent Storage drive.
- 2)** The next step is to right click on the **"C:\My Documents"** folder on the desktop, choose **"Properties"** and change the **"target folder location"** to point to the new folder that you set up. Select the **"OK"** button once you have made the change.
- 3)** Next, you need to move the content of **"C:\My Documents"** (which you will now have to access via the **C:\** drive in **"My Computer"**) to the new folder (which you can access via **"My Documents"** on the desktop).
- 4)** The final step is to delete **"My Documents"** from the **C:\** drive to avoid confusion.

## Moving your Internet "Favorites" Folder

As long as you use Windows Explorer to move the Favorites folder, Windows will update the internal fields that identify it. Suppose the current Favorites folder is **C:\Windows\Favorites**. Right-drag this folder to the location you want to use instead, and choose Move here from the menu that pops up when you drop the folder.

Otherwise you can edit the registry and navigate to:

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\U  
ser Shell Folders**

In the right-hand pane, the value named Favorites should contain the full path for the Favorites folder. Double-click it and change it to the correct location.

## Moving Important Information in Outlook

Microsoft Outlook uses **.pst** files (**Outlook.pst** and **archive.pst**) to store your sent mail, address book, and other Outlook specific information. The following steps describe the process needed to relocate your **.pst** files from their current location to the unprotected,

persistent storage partition. This makes it possible for a user to persistently save information pertaining to Outlook while their system is in a protected state.

- 1) Close down Outlook.
- 2) Open "**My Computer**" and select "**Folder Options**" from the **Tools** menu
- 3) Select the **View** tab and make sure "**Show hidden files**" and folders is selected. Click "**OK**".
- 4) Navigate to **C:\Documents and Settings\\Local Settings\Application Data\Microsoft\Outlook\**  
Copy the files "outlook.pst" and "archive.pst" from there to your persistent storage drive or a folder in the persistent storage drive. *Note: There may be similarly-named files which also contain a number. Copy these as well.*
- 5) Right-click on the Outlook icon on the desktop and select "**Properties**".
- 6) Click on the "**Data Files**" button.
- 7) For each entry on the list corresponding to the copied files, select it and click on "**Settings**".
- 8) Outlook will complain that the file cannot be found, and ask you to locate it. Select the file with that name from the ones you copied to your persistent storage partition.

# Glossary

**Activation Number**—when registering manually, this is the registration number Cornerstone will read from a file.

**BIOS**—the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices. The BIOS is stored in read-only memory (ROM) so that it can be executed when you turn on the computer. Although critical to performance, the BIOS is usually invisible to computer users. Cornerstone does not protect your systems BIOS.

**Centurion Web**—refers to Centurion Technologies' web servers used for licensing and updates.

**CompuGuard Control Center (CCC)**—a remote management application used to control CompuGuard Cornerstone and other Centurion client machines.

**"Delayed Write Failed"**—is an error that will occur when your system is writing to Cornerstone's temporary storage area while it is full. Increasing the size of the temporary storage area will often eliminate this error.

**Disabled**—(unprotected) most often refers to Cornerstone's protection status. When Cornerstone is disabled it is not protecting your machine. All changes made to a system while Cornerstone is disabled will be permanent (unless the Oops! command is run)

**Enabled**—(protected) most often refers to Cornerstone's protection status. When Cornerstone is enabled it is protecting your machine from all configuration changes.

**GUI**—an acronym for Graphical User Interface. A GUI is what the user sees and uses to manipulate an application.

**Hotkey**—a pre-defined key combination used to display the green Cornerstone shield in the Taskbar. When protection is enabled and Cornerstone is running in Stealth Mode it is required that you enter the hotkey before disabling protection locally. The default hotkey is: Ctrl + Alt + F10.

**IP Address**—A 32-bit address used to identify a node on an IP network. Each node on the IP network must be assigned a unique IP address, which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). IP Addresses can either be statically (will not change) or dynamically (will periodically change) assigned.

**Mount**—Cornerstone allows you to create a persistent storage area that is treated like a drive. Once the storage area is created, mounting it will make it available to the user.

**Next Boot Protection Mode**—is defined as disabled (unprotected) or enabled (protected). It is the protection status of a machine when it is rebooted. It can be the same or the opposite of the "Current" protection status.

**Oops!**—a command that allows you to changed the protection status without rebooting your machine. Running the Oops! command, will change the protection status since the last boot. You can choose to allow or disallow the use of this command.

**Order Number**—the number provided to you by Centurion Technologies when you purchased licenses. Each order number is linked to a certain purchase and is used when licensing Cornerstone software on a machine.

**Persistent Storage Area**—an area created by Cornerstone to allow users to permanently save data while protection is enabled. This area is given a name, assigned a drive letter, configured to a size. Data saved on the persistent storage drive will remain on a system even when the machine is rebooted from a protected state.

**Port**—A connection point on your computer where you can connect devices that pass data into and out of a computer. In order for Cornerstone to be managed by the CCC it must be configured to the same port number as the CCC. The default port number for both is 25555.

**Protection Mode**—is defined as disabled (unprotected) or enabled (protected). Can refer to the "Current" protection mode or the "Next Boot" protection mode.

**Registry**—A database repository for information about a computer's configuration. The registry contains information that Windows continually references during operation.

**Server Name**—the identifier of a computer on your network provided by software components such as Domain Name System (DNS) or Windows Internet Name Service (WINS). These components dynamically map IP Addresses to computer names. This allows users to access resources by name instead of requiring them to use IP addresses that are difficult to recognize and remember. The server name, or computer name, is required when remotely managing Cornerstone with the CCC. If the CCC is running on a computer with a dynamically assigned IP Address, it is best to configure Cornerstone to the CCC's computer name.

**Stealth Mode**—when enabled, the CompuGuard Cornerstone icon will not be visible to a user. When disabled, the Cornerstone icon will be visible to a user. Stealth Mode will only affect the Cornerstone's icon when protection is enabled.

**TCP/IP**—(Transmission Control Protocol/Internet Protocol) is a set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

**Temporary Storage Area**—is an area on the hard drive used by Cornerstone to read and write changes to a system. This area is created on all drives protected by Cornerstone and can be resized. The temporary storage area on the system drive must be a minimum of 350MB.

**Unmount**—unmounting a persistent storage area/drive will make the drive and all its contents unavailable to the user. The drive and its contents still exist, but cannot be used until it is mounted.

**USB**—(Universal Serial Bus) An external bus that supports Plug and Play installation. Using USB, you can connect and disconnect devices without shutting down or restarting your computer. Cornerstone allows you to block reading from and writing to all connected USB storage devices. USB Blocking is either "enabled" or "disabled"

**Wake-On-LAN**—(WOL) is the ability to switch on remote computers through special network packets. This only works with network cards and motherboards that are Wake-On-LAN compliant. The CCC is able to send WOL commands to its Centurion clients.

## **Technical Support**

To get technical support or sales information for CompuGuard Cornerstone, please contact Centurion Technologies, Inc. at the following links:

Web: [www.centuriontech.com](http://www.centuriontech.com)

E-mail for technical support: [support@centuriontech.com](mailto:support@centuriontech.com)

E-mail for sales information: [sales@centuriontech.com](mailto:sales@centuriontech.com)

Sales: 1-800-224-7977

Technical Support: 1-888-265-6055

# **License Agreement**

## **SOFTWARE LICENSE, LIMITED WARRANTY AND LIMITATION OF LIABILITY AGREEMENT**

### **IMPORTANT NOTICE; READ CAREFULLY:**

This License for Customer Use of Centurion Technologies™ software is the agreement which governs use of the software of Centurion Technologies, Inc. and associated printed materials ('Software.'). By downloading, installing, copying or otherwise using the Software, you agree to be bound by the terms of this License Agreement. If you do not agree to the terms of this License Agreement, do not download, install, copy or otherwise use the Software.

### **RECITALS**

The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is not sold, and instead is only licensed for use, strictly in accordance with this document.

### **GRANT OF LICENSE**

Rights and Limitations of Grant. Centurion Technologies hereby grants Customer the following non-exclusive, non-transferable right to use the Software, with the following limitations:

Rights. Customer may install the Software and use for evaluation purposes for up to 30 days. Upon expiration of the 30 days, the customer must register software with a purchased license or uninstall from the computer. Except for making one back-up copy of the Software, may not otherwise copy the Software.

Limitation. No Reverse Engineering. Customer may not reverse engineer, decompile or disassemble the Software, nor attempt in any other manner to obtain the source code.

No Separation of Components. The Software is licensed as a single product. Its component parts may not be separated or used separately from the other parts.

No Rental. Customer may not rent or lease the Software to someone else.

### **COMPLIANCE OF LICENSES**

Customer agrees to use any and all Software in conformity with your valid licenses from Centurion and acknowledges Centurion may collect machine IP and MAC addresses and hard drive serial identification numbers to enforce licensing.

### **CONSUMER INFORMATION AND PRIVACY**

For details about Centurion's privacy policies, please refer to the Centurion Privacy Policy contained on a Web site designated by Centurion. You agree to be bound by the applicable Centurion privacy policies.

### **TERMINATION**

This License Agreement will automatically terminate if Customer fails to comply with any of the terms and conditions hereof. In such event, Customer must destroy all copies of the SOFTWARE and all of its component parts.

**COPYRIGHT**

All title and copyrights in and to the Software (including but not limited to all images, photographs, animations, video, audio, music, text, and other information incorporated into the Software), the accompanying printed materials and any copies of the Software, are owned by Centurion Technologies. The Software is protected by copyright laws and international treaty provisions. Accordingly, Customer is required to treat the Software like any other copyrighted material, except as otherwise allowed pursuant to this License Agreement and that it may make one copy of the Software solely for backup or archive purposes.

**End-User License Agreement****APPLICABLE LAW**

This agreement shall be deemed to have been made in, and shall be construed pursuant to, the laws of the State of Missouri.

**DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY**

No Warranties. To the maximum extent permitted by applicable law, the software is provided 'as is' and Centurion Technologies disclaims all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose.

No liability for consequential damages. To the maximum extent permitted by applicable law, in no event shall Centurion Technologies be liable for any special, incidental, indirect, or consequential damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the software, even if Centurion Technologies has been advised of the possibility of such damages.

No warranty against infringement. There is no warranty that the use of the software will not infringe any third party patents, copyrights, trademarks, or other rights

Other Limitations. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply. If the foregoing limitation of liability is not enforceable and if a court of competent jurisdiction in a final, non-appealable judgment finds the Software licensed to Customer to be defective and to have directly caused bodily injury, death, or property damages, in no event shall Centurion Technologies' liability exceed the greater of \$1,000.00 or the price paid for the License Agreement of the Software that caused the damage. Customer acknowledges that the applicable license fee for the Software reflects this allocation of risk.

**MISCELLANEOUS**

If any provision of this License Agreement is inconsistent with, or cannot be fully enforced under, the law, such provision will be construed as limited to the extent necessary to be consistent with and fully enforceable under the law. This agreement is the final, complete and exclusive agreement between the parties relating to the subject matter hereof, and supersedes all prior or contemporaneous understandings and agreements relating to such subject matter, whether oral or written. Customer agrees that it will not ship, transfer or export the Software into any country, or use the Software in any manner, prohibited by the United States Bureau of Export Administration or any export laws, restrictions, or regulations. This License Agreement may only be modified in writing signed by an authorized officer of Centurion Technologies.