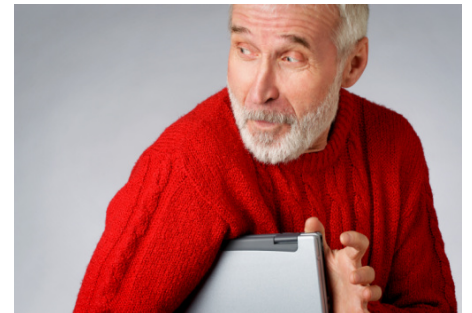




The CyberAngel® Encryption & Tracking Software

Cutting Edge Security Solutions for Business & Consumer Markets



The CyberAngel® Software User Guide

The CyberAngel[®] Security Software Overview

This User Guide is intended to assist you with the general understanding of The CyberAngel[®] with Wi-Trac. It covers all phases of the installation process, normal operations, common support issues and known error codes and recommended solution paths. We find that with proper pre-installation planning and configuration, end-user support is minimal on the back end. This guide can help ensure a smooth implementation and operation of The CyberAngel[®] with Wi-Trac software within your organization, and a valuable resource tool for your Help Desk staff.

Laptop theft—and how to recover from it, should it happen to you— is a major concern for everyone: corporations, consumers, higher education, non-profits, and government. The CyberAngel[®] with Wi-Trac is a unique “hybrid” solution combining Data Encryption, User Authentication, and Tracking / Recovery in a single and easily implemented solution. With strong industry approved (and exportable) encryption, The CyberAngel[®] with Wi-Trac addresses Privacy Acts and recent Security Breach Notification Laws, which have enormous notification costs, liability costs, and the loss of customers / clients / patients. Custom configured for each client, The CyberAngel[®] with Wi-Trac can be triggered by a two-factor authentication or integrate with existing Windows or Novell passwords and other authentication devices. If the authentication is violated, sensitive data and applications (such as a VPN client, financial application or client database) are encrypted and hidden from the unauthorized user, communication ports are blocked, and a covert signal is sent to the CyberAngel Security Monitoring Center. After capturing the location of the computer, we will immediately send a real-time notification to the registered user or organization informing them of the unauthorized attempt to access that computer. Our Recovery Team will work with local Law Enforcement and the ISP’s to facilitate recovery of your stolen computer, and act a liaison between you and law enforcement until a successful resolution.

In today’s high-risk environment, everyone is concerned with security and the liability of not providing enough security to clients and employees. Fines, fees, and data loss are only part of the picture. Organizations that experience a public breach also experience nearly 20% customer/client attrition. Encryption and recovery is the best “safe harbor” according to Breach Notification Laws in most states

The CyberAngel[®] with Wi-Trac protects your data, your computers, your reputation.



Pre-Installation on Microsoft XP

Service Pack 2

The operating system must have at least Service Pack 2 for Microsoft Windows XP Professional / Home.

.NET Framework 2.0 or higher

The .NET Framework 2.0 can be received through Windows Update. Most of The CyberAngel® with Wi-Trac components will NOT run without this update.

Logged on as Local Admin of the machine

To ensure proper installation of all services and modules of The CyberAngel® with Wi-Trac make sure you are logged on as the local Administrator and not the Domain Administrator or other User groups.

Residing files from Evaluation or prior installation

If The CyberAngel® with Wi-Trac was installed for evaluation or are updating current version to a newer version some files need to be removed. The files that will reside on the computer after using the configuration manager and running uninstall are:

protected.sdsk = C:\Protected.Sdsk
mscae32.log = C:\mscae32.log
dsn1002.ca = C:\dsn1002.ca
sdwlib.dll = C:\WINDOWS\System32\sdwlib.dll
optic32.dll = C:\WINDOWS\System32\optic32.dll
sdwmap32.exe = C:\WINDOWS\System32\sdwmap32.exe

A simple right-click and delete will remove these files.

Pre-Installation on Microsoft Vista

Logged on as Administrator or Admin Group

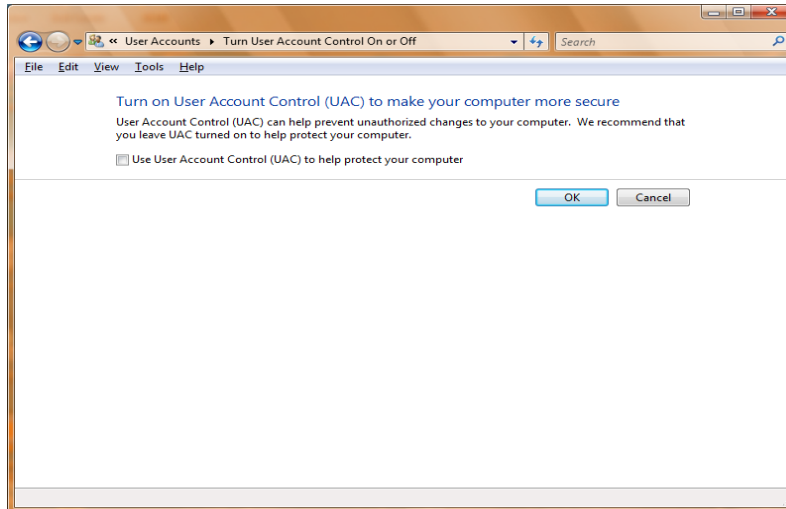
With Vista there is an Administrator Group and "The Administrator", being logged on as either one of these will work.

.NET Framework 2.0 or higher

The .NET Framework 2.0 can be received through Windows Update. Most of The CyberAngel® with Wi-Trac components will NOT run without this update.

UAC disabled

To install The CyberAngel® with Wi-Trac properly onto a Vista operating system the User Account Control feature should be disabled. This can be accomplished by going to the Control Panel\User Accounts\Turn User Account Control on or off.



Residing files from Evaluation or prior install

If The CyberAngel[®] with Wi-Trac was installed for evaluation or are updating current version to a newer version some files need to be removed. The files that will reside on the computer after using the configuration manager and running uninstall are:

protected.sdsk = C:\Protected.Sdsk
mscae32.log = C:\mscae32.log
dsn1002.ca = C:\dsn1002.ca
sdwlib.dll = C:\WINDOWS\System32\sdwlib.dll
optic32.dll = C:\WINDOWS\System32\optic32.dll
sdwmap32.exe = C:\WINDOWS\System32\sdwmap32.exe

A simple right-click and delete will remove these files.

Technical Considerations

Connection to the Internet

Make sure you have established a connection to the internet before performing the installation process.

Establish connection path to the CyberAngel Security Monitoring Servers

If you can ping 63.243.65.1 then you should be able to register.

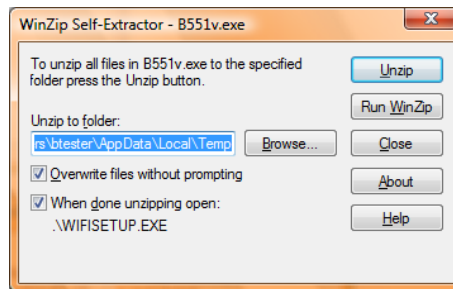
Make adjustments to Firewall if needed

Some hardware firewalls may require port 80/HTTP to allow two-way traffic from our domain to that computer on their domain for proper registration. Contact Technical Support for assistance **1-800-501-4344**.

Installation on Microsoft XP

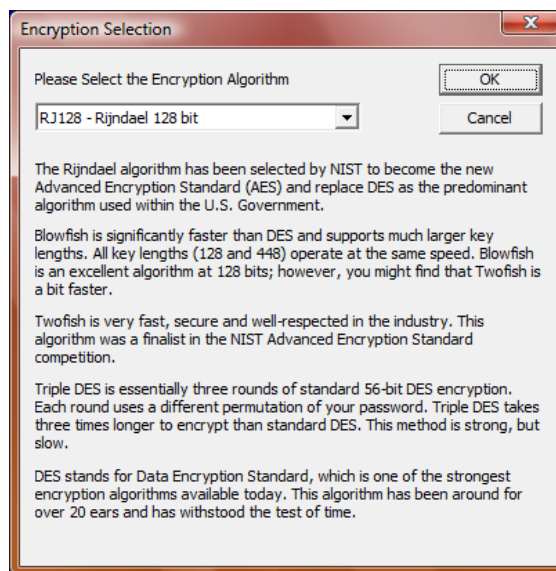
From CD with self-extracting executable

Simply run the application on the CD named **Bxxx.EXE** to get started (Bxxx=build number-i.e B478.exe). A WinZip Self-Extractor window will appear, click the UnZip button. This will start the installation of The CyberAngel® with Wi-Trac. The default “un-zip to folder” location when this windows pops up is recommended for the installation process.



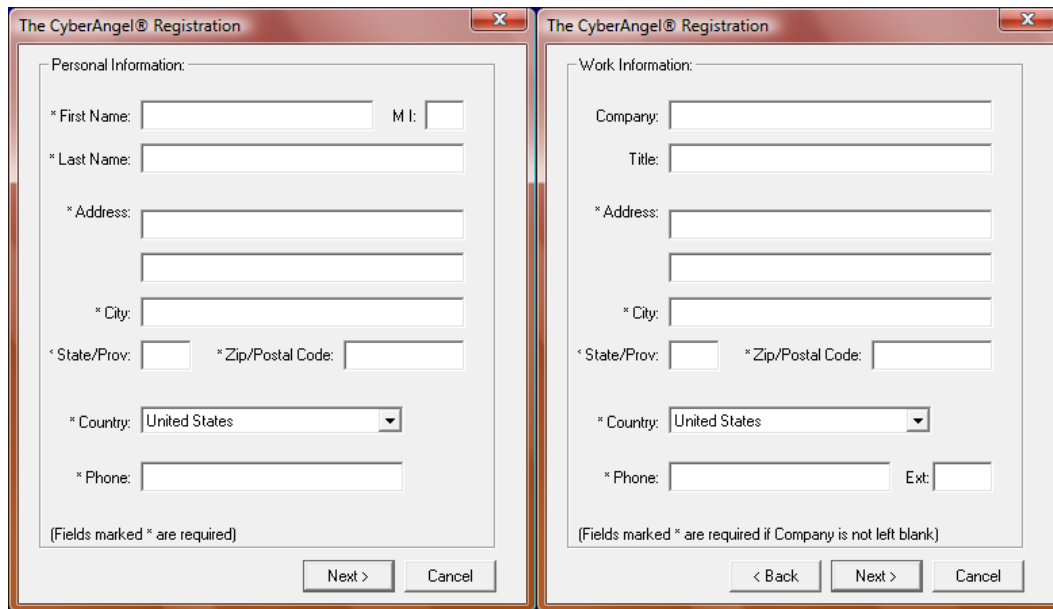
Encryption Algorithm

This is where you can choose various algorithms to encrypt your data once installed. Most configuration come pre-selected from when the order was placed and the choice of another algorithm will not be present.



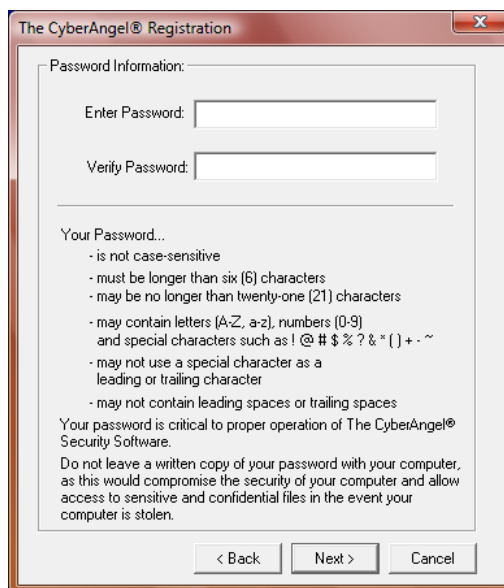
User Information/Customer Information

The User Information section is where you will want to input the individual who will be using the computer that you're installing The CyberAngel® with Wi-Trac on. The Customer Information section is usually preloaded with information The CyberAngel® with Wi-Trac received during the initial order.



Password

The selection of a password is needed for proper authentication when using The CyberAngel® with Wi-Trac in the Two-Factor Authentication mode or when accessing the Configuration Manager.



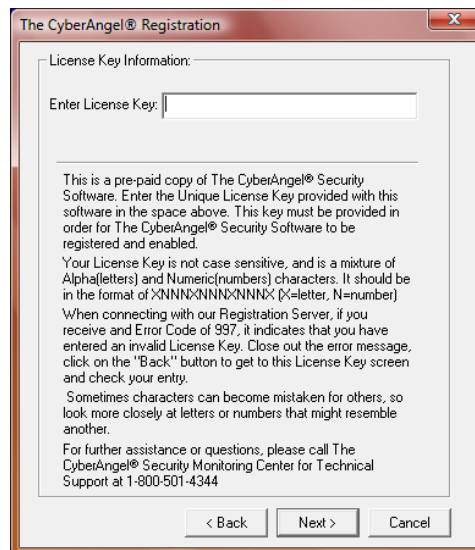
Authentication Code

The Authentication Code is a unique identifier for each individual computer that you assign. The Authentication Code will be used when calling the CyberAngel Security Monitoring Center for technical support for verification purposes. It can also be a global code to identify any Help Desk staff authorized to work on any end-user accounts.



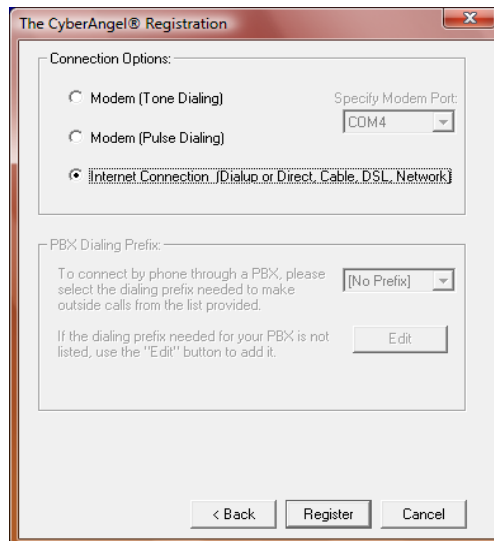
License Key

A listing of License Keys is provided with the documentation sent when shipping The CyberAngel® with Wi-Trac software. For larger orders, a list of the keys will be located on the CD of the software as well (i.e. ACME 57343.txt). This list and Master CD should be kept safe and accessible for future installations. License reports can be obtained upon request from our Security Monitoring Center.



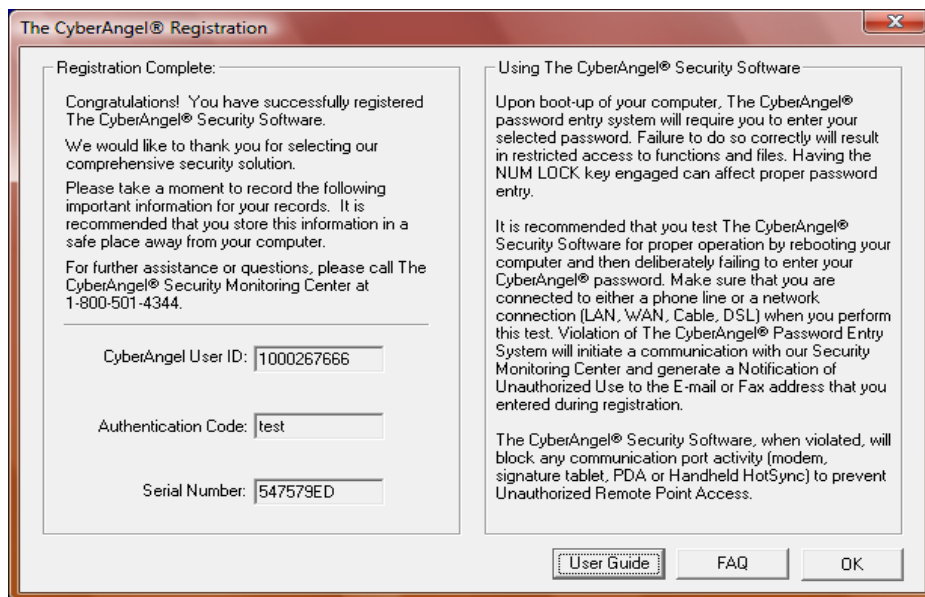
Connection Selection

The most common selection in this section will be “Internet Connection” and this is for all connections, DSL, WiFi, Cable, to the internet except a 56K modem, aka, telephone line.



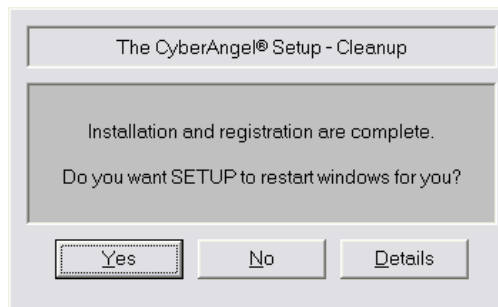
CyberAngel User ID Number

The Cyberangel User ID number is a unique identifier for each individual installation of The CyberAngel[®] with Wi-Trac. If The CyberAngel[®] with Wi-Trac is uninstalled then re-installed; another CyberAngel User ID Number will be assigned. Using this unique identifier in a database for asset management with the computer name, Authentication Code, License Key, etc. is recommended.



Reboot after initial install

Once the registration has completed you will then be asked to “Reboot” your machine. Once you have logged back into Windows wait for The CyberAngel[®] with Wi-Trac password prompt to appear, if you have two-factor authentication enabled. If you have the authentication set to “Fully” then the Windows logon window will be used for authentication. If in “Two-Factor” mode then you must not click on anything or anywhere, for this will violate The CyberAngel[®] with Wi-Trac password prompt and generate an alarm and will not create the “Protected” drive correctly. If in “Fully” you don’t have to wait. The “Protected” drive will be created after entering the correct Windows password.



Creating/Mapping of “Protected” drive

The “Creating” of the “Protected” drive is only done after the initial reboot. Logon to Windows normally and wait for the CyberAngel Logon. Enter The CyberAngel[®] with Wi-Trac password created during registration, wait 2 minutes, then reboot. This is to allow the computer to apportion the Protected Secure Drive area properly. This is a one time occurrence and no performance lag should be noted on subsequent reboots

Send alarm and verify with Monitor Center

To verify your installation was successful you can violate the Windows logon, for “Fully” authentication mode, and The CyberAngel[®] with Wi-Trac password prompt when in “Two-Factor” authentication mode. You can call technical support to ensure the alarm was received. **NOTE:** You should only do this on the second reboot, for the first reboot is the only time it creates the “Protected” drive.

Installation on Microsoft Vista

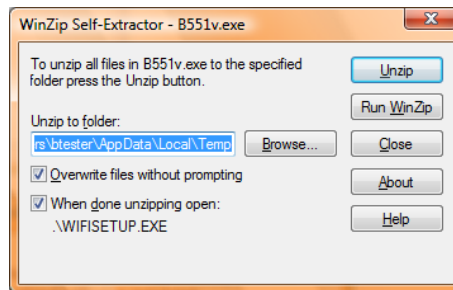
Vista User Account Control (UAC)

The security architecture within Microsoft Vista interacts differently with software applications than previous Microsoft operating systems.

The User Account Control (UAC) is a security feature of Microsoft Vista that displays a permission prompt asking if the user would like to execute the software application. ***UAC must be disabled for The CyberAngel with Wi-Trac to install properly.*** Once The CyberAngel with Wi-Trac is installed, UAC may be re-enabled.

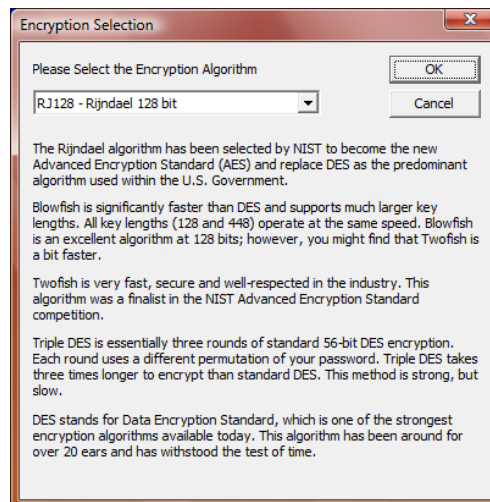
From CD with self-extracting executable

Simply run the application on the CD named **Bxxx.EXE** to get started (Bxxx=build number-i.e B478.exe). A WinZip Self –Extractor window will appear, click the UnZip button. This will start the installation of The CyberAngel® with Wi-Trac. The default “un-zip to folder” location when this windows pops up is recommended for the installation process.



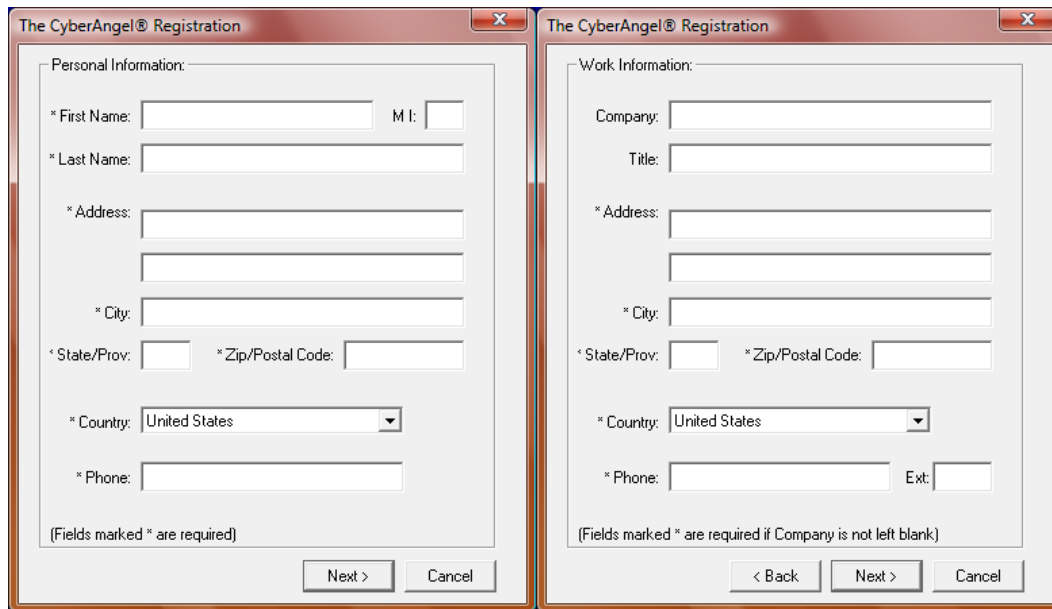
Encryption Algorithm

This is where you can choose various algorithms to encrypt your data once installed. Most configuration come pre-selected from when the order was placed and the choice of another algorithm will not be present.



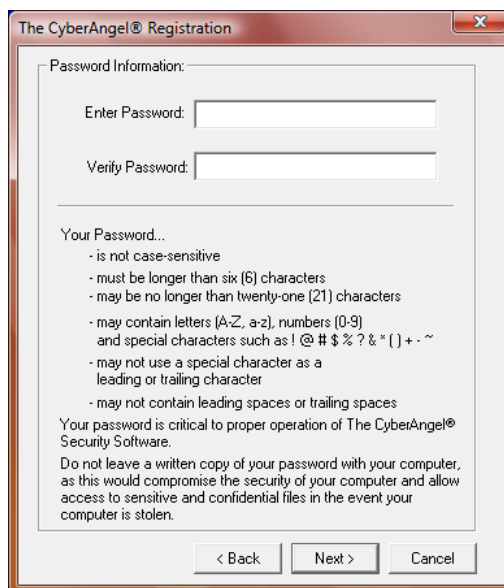
User Information/Customer Information

The User Information section is where you will want to input the individual who will be using the computer that you're installing The CyberAngel® with Wi-Trac on. The Customer Information section is usually preloaded with information The CyberAngel® with Wi-Trac received during the initial order.



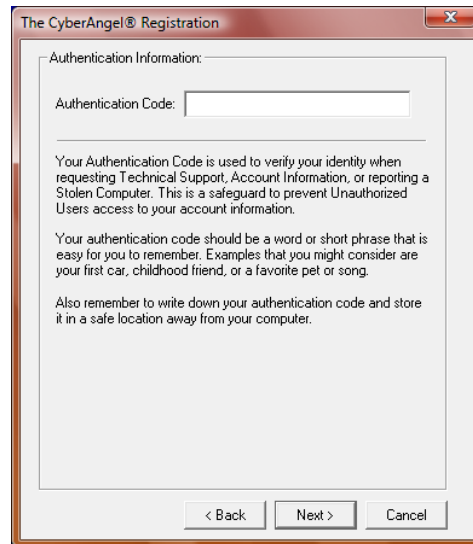
Password

The selection of a password is needed for proper authentication when using The CyberAngel® with Wi-Trac in the Two-Factor Authentication mode or when accessing the Configuration Manager.



Authentication Code

The Authentication Code is a unique identifier for each individual computer that you assign. The Authentication Code will be used when calling the CyberAngel Security Monitoring Center for technical support for verification purposes. It can also be a global code to identify any Help Desk staff authorized to work on any end-user accounts.



The CyberAngel® Registration

Authentication Information:

Authentication Code:

Your Authentication Code is used to verify your identity when requesting Technical Support, Account Information, or reporting a Stolen Computer. This is a safeguard to prevent Unauthorized Users access to your account information.

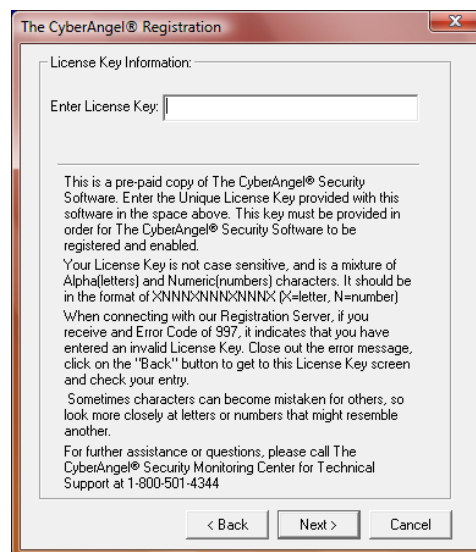
Your authentication code should be a word or short phrase that is easy for you to remember. Examples that you might consider are your first car, childhood friend, or a favorite pet or song.

Also remember to write down your authentication code and store it in a safe location away from your computer.

< Back Next > Cancel

License Key

A listing of License Keys is provided with the documentation sent when shipping The CyberAngel® with Wi-Trac software. For larger orders, a list of the keys will be located on the CD of the software as well (i.e. ACME 57343.txt). This list and Master CD should be kept safe and accessible for future installations. License reports can be obtained upon request from our Security Monitoring Center.



The CyberAngel® Registration

License Key Information:

Enter License Key:

This is a pre-paid copy of The CyberAngel® Security Software. Enter the Unique License Key provided with this software in the space above. This key must be provided in order for The CyberAngel® Security Software to be registered and enabled.

Your License Key is not case sensitive, and is a mixture of Alpha(letters) and Numeric(numbers) characters. It should be in the format of: XNNNXXNNNXXNNNXX (X=letter, N=number)

When connecting with our Registration Server, if you receive an Error Code of 997, it indicates that you have entered an invalid License Key. Close out the error message, click on the "Back" button to get to this License Key screen and check your entry.

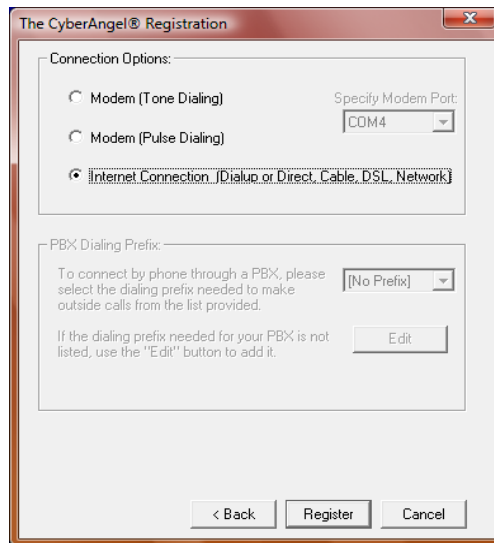
Sometimes characters can become mistaken for others, so look more closely at letters or numbers that might resemble another.

For further assistance or questions, please call The CyberAngel® Security Monitoring Center for Technical Support at 1-800-501-4344

< Back Next > Cancel

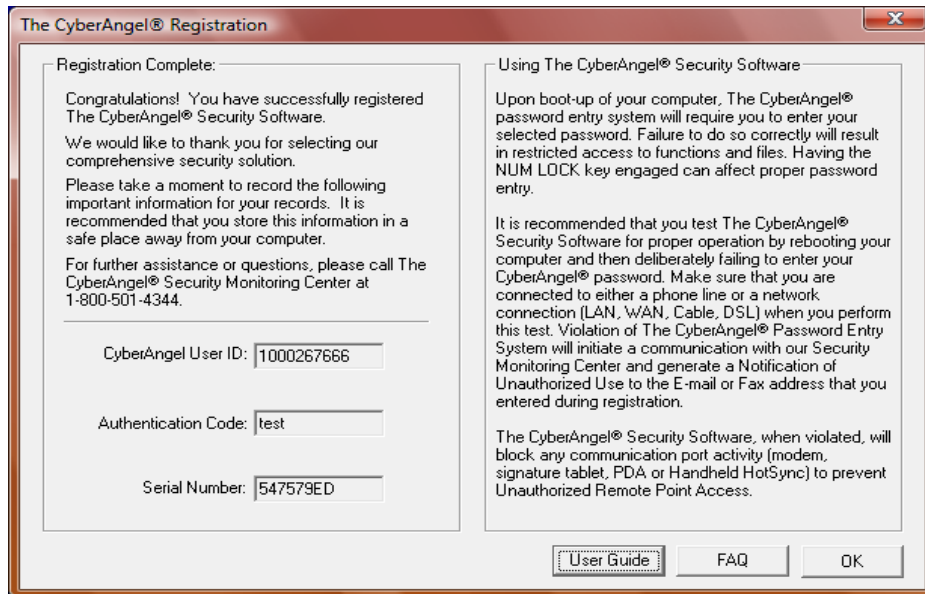
Connection Selection

The most common selection in this section will be “Internet Connection” and this is for all connections, DSL, WiFi, Cable, to the internet except a 56K modem, aka, telephone line.



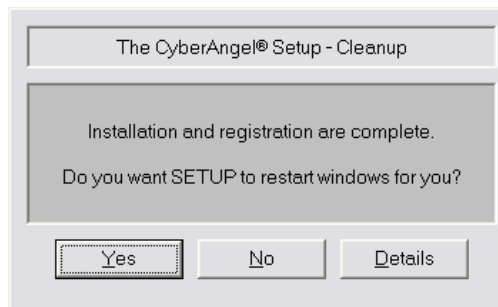
CyberAngel User ID Number

The Cyberangel User ID number is a unique identifier for each individual installation of The CyberAngel[®] with Wi-Trac. If The CyberAngel[®] with Wi-Trac is uninstalled then reinstalled; another CyberAngel User ID Number will be assigned. Using this unique identifier in a database for asset management with the computer name, Authentication Code, License Key, etc. is recommended.



Reboot after initial install

Once the registration has completed you will then be asked to “Reboot” your machine. Once you have logged back into Windows wait for The CyberAngel[®] with Wi-Trac password prompt to appear, if you have two-factor authentication enabled. If you have the authentication set to “Fully” then the Windows logon window will be used for authentication. If in “Two-Factor” mode then you must not click on anything or anywhere, for this will violate The CyberAngel[®] with Wi-Trac password prompt and generate an alarm and will not create the “Protected” drive correctly. If in “Fully” you don’t have to wait. The “Protected” drive will be created after entering the correct Windows password.



Creating/Mapping of “Protected” drive

The “Creating” of the “Protected” drive is only done after the initial reboot. Logon to Windows normally and wait for The CyberAngel[®] with Wi-Trac Logon. Enter The CyberAngel[®] with Wi-Trac password created during registration, wait 2 minutes, then reboot. This is to allow the computer to apportion the Protected Secure Drive area properly. This is a one time occurrence and no performance lag should be noted on subsequent reboots

Send alarm and verify with Monitor Center

To verify your installation was successful you can violate the Windows logon, for “Fully” authentication mode, and The CyberAngel[®] with Wi-Trac password prompt when in “Two-Factor” authentication mode. You can call technical support to ensure the alarm was received. **NOTE:** You should only do this after your second reboot, the first reboot after registration is for the creation of the “Protected” drive, and the authentication should not be violated during the .

Post Installation on Microsoft XP

Understanding the Windows logon

The Windows logon window is for logging on to the operating system using the required credentials, such as, username and password. With The CyberAngel[®] with Wi-Trac installed on the machine and the user violates this logon three times it will send the Monitoring Center an alarm event. If the User sits at this prompt too long it will also generate an alarm event. This is called the “Failsafe” feature.

Understanding the CyberAngel prompt

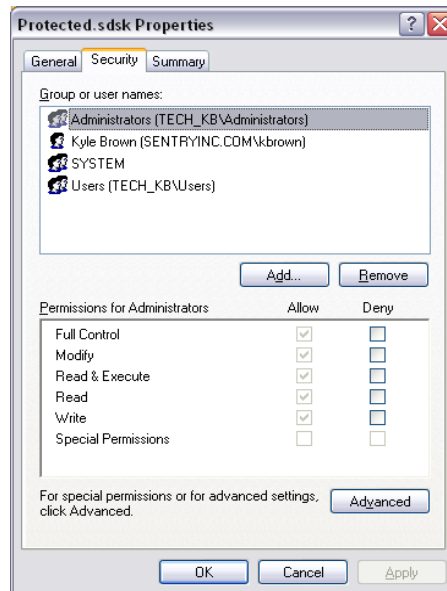
The CyberAngel[®] with Wi-Trac password prompt will only be visible if the current configuration is set to “Fully” authentication mode. When violating this prompt the computer communication ports are blocked making them inaccessible. This also generates an alarm and an e-mail stating the unauthorized access and the CyberAngel User ID number associated with that computer will be sent to the predefined account.

Checking for the “Protected” drive

You can verify that the “Protected” drive was created successfully after authentication. Simply go into My Computer and verify there is another drive with the label “Protected”. It can take several seconds sometimes, depending on the machine, for the “Protected” drive to become mapped and visible.

Permission issues for non-Admin users

If the end-user The CyberAngel[®] with Wi-Trac was installed for does not have Admin rights, then the Administrator must give Read and Write access to the protected.sdsd file located in the C:\. To do this simply right-click the file and choose “Properties” then the “Security” tabs and add the user to the list along with a check mark for Read & Write permissions.



If you do not see a Security Tab, go to My Computer\Tools\Folder Options\View Tab\Advanced Settings, and then uncheck the “Use Simple File Sharing” box. You should then be able to follow the process above

Registry Permissions

To check / change permissions within the Registry, you will need to right-click the PC Dynamics folder located under; HKEY_LOCAL_MACHINE\Software\PC Dynamics, and choose permissions. Here you will add the current user to the list along a check mark on the Read and Write permissions.

CyberAngel User ID number and Authentication Code

The CyberAngel User ID Number (i.e. 1000249535) and the Authentication Code are unique identifiers for each individual installation. When contacting Technical Support, you will be asked for the Authentication Code either chosen at registration or during pre-configuration for identification purposes. Often, an Authentication Code will be selected for Help Desk staff to use to manage end-user accounts. This Authentication Code lets our staff know that they are authorized to access / edit / inquire about end user accounts. The CyberAngel User ID number can be used as well as the User Name for querying purposes.

Post Installation on Microsoft Vista

Understanding Credential Tiles

The Credential Tiles identify different users / rights setup for logging onto a specific computer. Once you click on a Credential Tile, you will be asked for a username and password. Violation of this logon will generate an alarm event. Failure to enter anything at this logon for a specified period of time will initiate the "Failsafe Alarm" feature.

Using the "Run As Administrator"

If needing to access The CyberAngel® with Wi-Trac Configuration Manager, and the user is logged in as part of the Administrator Group, then he/she must right-click on the CONFIG.EXE file and choose "Run as Administrator" to have Administrator privileges. The failure to do so will cause the changed attempted to make will not be valid.

User Account Controls

The User Account Control (UAC) is a security feature of Microsoft Vista that displays a permission prompt asking if the user would like to execute the software application. ***UAC must be disabled for The CyberAngel with Wi-Trac to install properly.*** Once The CyberAngel® with Wi-Trac has been installed; you can turn the UAC feature within Windows back on. However, UAC will ask you each time The CyberAngel® with Wi-Trac loads if you want to run that application. This will not affect The CyberAngel® with Wi-Trac's daily operation.

Checking for the "Protected" drive

You can verify that the "Protected" drive was created successfully after authentication. Simply go into My Computer and verify there is another drive with the label "Protected". It can take several seconds sometimes, depending on the machine, for the "Protected" drive to become mapped then visible.

CyberAngel User ID number and Authentication Code

The CyberAngel User ID Number (i.e. 1000249535) and the Authentication Code are unique identifiers for each individual installation. When contacting Technical Support, you will be asked for the Authentication Code that was chosen at registration or during pre-configuration for identification purposes. Often, an Authentication Code will be selected for Help Desk staff to use to manage end-user accounts. This Authentication Code lets our staff know that they are authorized to access / edit / inquire about end user accounts. The CyberAngel User ID number can be used as well as the User Name for querying purposes.

The CyberAngel Software Normal Operation

The Windows / Network / Novell login window is for logging on to the operating system using the required credentials, such as User Name and Password. With The CyberAngel with Wi-Trac installed, and if a user violates this logon three times, it will send an alarm to the CyberAngel Security Monitoring Center and an e-mail notification stating that there has been an unauthorized access attempt will be sent to the notification address designated during configuration /registration. If the user sits too long at this logon prompt it will also generate an alarm, a “failsafe” signal for someone possibly trying to access that computer. Notifications like these, unless the computer has been reported stolen, can be used as asset tracking reports, but should be purged regularly from the mailbox to which they are sent. A record of all communication activity from a protected computer to the CyberAngel Security Monitoring Center is kept in our Database Management System for archive purposes.

Once the end-user successfully logs onto their computer using their normal Windows / Network / Novell logon, the computer desktop will load. A secondary password prompt will appear, and once the selected CyberAngel password is entered successfully, they will have full access to that machine and its resources. If the secondary password prompt is violated 3 times, or the mouse is clicked on anything outside of the password box before password entry, an alarm event will be initiated to our Security Monitoring Center.

A Secure Drive (P) will be created, and is where all confidential or sensitive data should be stored. VPN Clients and other communication applications can also be placed within the Secure Drive to help prevent unauthorized Remote Access attempts. When that logon is violated, the data within the Secure Drive will be encrypted with the encryption algorithm selected, and will be hidden from view. COM Ports will also be locked from the unauthorized user. A notification of unauthorized access attempt will be generated to the recipient designated in the Configuration Chart or selected during registration.

Should a user violate their logon, and restrict themselves from the Secure Drive and the applications and data stored within, they would simply need to reboot and properly enter their Windows / Network / Novell logon then the secondary CyberAngel password to regain full access to their machine. Only if that computer has been reported stolen will authorities be contacted when an alarm event is generated.

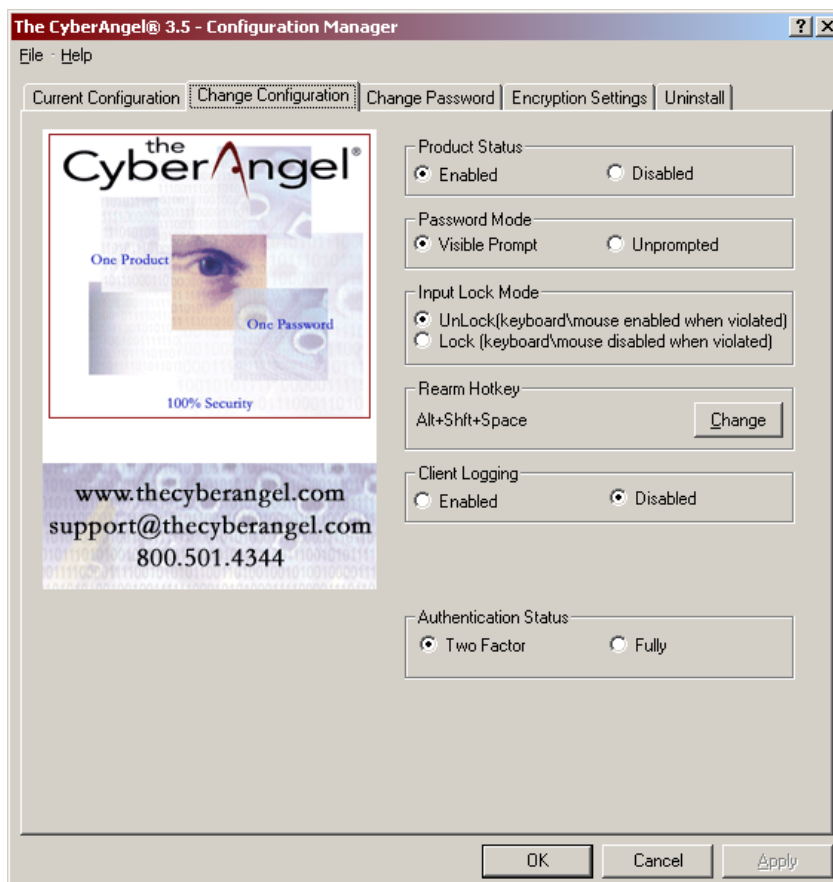
Stolen Computer Reporting & Recovery

If a computer is stolen, the client / end-user is responsible for reporting that theft to the proper authorities. They then should contact our CyberAngel Security Monitoring Center at **800.501.4344** and a Support Technician will flag that computer as stolen. Any additional changes in notification paths or special notification procedures will be discussed and decided upon at that time. A police report number, contact name and number for that local law enforcement agency that the theft was reported to, will be required in order for our Recovery Team to properly liaise with those enforcement officials. Also, computer type and serial number will be needed to help in the positive identification of that stolen computer. When we do receive an alarm from that reported stolen computer, we will compile all of the identification and location information, provide that to the law enforcement officials, and then contact the Client or other assigned individual with information about the recovery in progress.

The CyberAngel Software Configuration

Changing the Authentication Mode

- Run CONFIG.EXE located in C:\WINDOWS\System32\CONFIG.EXE
- Enter the CyberAngel password for that computer
- Select the tab “Change Configuration”
- Select Fully for Single Factor Authentication, or Two-Factor for Two-Factor Authentication
- Click on Apply, then OK, and then reboot your computer. Your change will now be in effect.

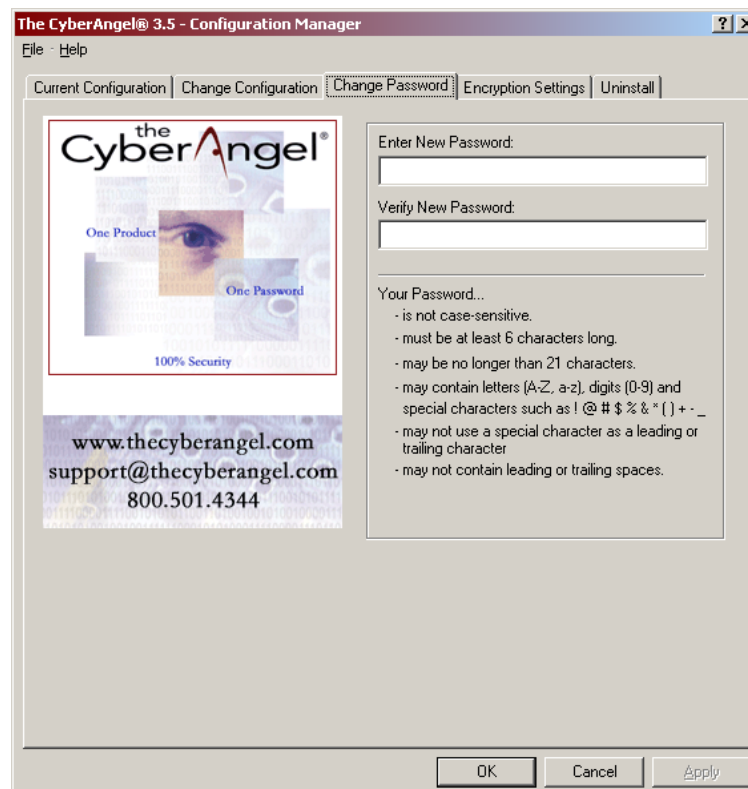


Changing the Password Mode

- Run CONFIG.EXE located in C:\WINDOWS\System32\CONFIG.EXE
- Enter the CyberAngel password for that computer
- Select the tab “Change Configuration”
- Select Unprompted for an invisible password prompt or Visible Prompt for a visible password prompt box
- Click on Apply, then OK, and then reboot your computer. Your change will now be in effect.

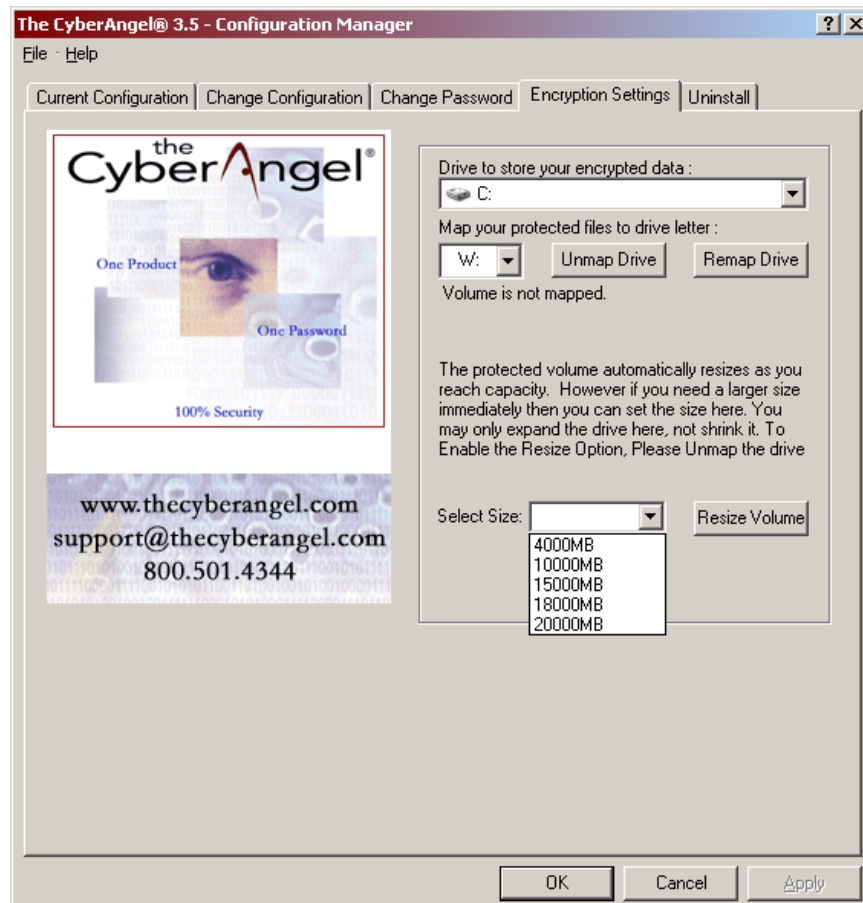
Changing The CyberAngel Password

- Run CONFIG.EXE located in C:\WINDOWS\System32\CONFIG.EXE
- Enter the CyberAngel password for that computer
- Select the tab “Change Password”
- Enter your new password here twice to verify
- Click on Apply, then OK, and then reboot your computer. Your change will now be in effect.



Changing the Secure Drive Size

- Run CONFIG.EXE located in C:\WINDOWS\System32\CONFIG.EXE
- Enter the CyberAngel password for that computer
- Select the tab “Encryption Settings”
- Wait until Volume is mapped. Then select Unmap Drive
- Select the size you wish to increase the Secure Drive to from the drop down menu.
- Click on Apply, wait until the hourglass returns to a normal mouse pointer...this might take a few minutes depending on the increase in size
- Select OK, and then reboot your computer. Your change will now be in effect.



Changing the Secure Drive Letter Designation

- Run CONFIG.EXE located in C:\WINDOWS\System32\CONFIG.EXE
- Enter The CyberAngel with Wi-Trac password for that computer
- Select the tab “Encryption Settings”
- Wait until volume is mapped. Then select “Unmap Drive”.
- Select the drive letter you wish the Secure Drive to map in the drop down menu.
- Click on “Apply”, select “OK”, then reboot your computer. Your change will now be in effect.

Changing the Secure Drive Letter Designation if Letter is Already Mapped

Some companies already have “P” mapped as a drive within their network. If this occurs, use the following procedure to change the Secure Drive to an available drive letter.

- Go to Start > Run > regedit. This will open the Registry Editor, with a left and right pane, and a scroll bar in the middle.
- Go to HKEY_CURRENT_USER > Software > PC Dynamics > Safehouse16 > Last Run.
- Left click on the Last Run folder. In the right pane, second line down says Map Drive. Right click > Modify
- A box will open with “P” in it. Change to the drive letter that you want to use, making sure it is in Caps. Click ok.
- Go back to the left pane. Click the “+” next to Last Run folder and you will see a folder named “A”.
- Left click the “A” folder. In the right pane, second line down says Map Drive. Right click > Modify. A box will open with “P” in it. Change to the drive letter that you want to use, making sure it is in Caps. Click ok.
- In the left pane, go back to the HKEY_CURRENT_USER and click on the “-“ and shrink it.
- Go to HKEY_LOCAL_MACHINE > Software > PC Dynamics > Safehouse16 > Last Run folder.
- Left click the Last Run folder. In the right pane, third line down says Map Drive. Right click > Modify. A box will open with “P” in it. Change to the drive letter that you want to use, making sure it is in Caps. Click ok.
- Close the registry editor with the **X** in the upper right corner.

Changing the Secure Drive Letter Designation for Dual Mapping (Win 2000 issue)

Some Windows 2000 machines will display dual protected drives, as a result of a Microsoft patch update. It will display the next available drive letter (E, F, G, etc.) as well as the “P” drive. Windows is forcing you to use that next available drive letter, and the following is the procedure to have it not show dual drives.

- Go to Start > Run > regedit. This will open the Registry Editor, with a left and right pane, and a scroll bar in the middle.
- Go to HKEY_CURRENT_USER > Software > PC Dynamics > Safehouse16 > Last Run.
- Left click on the Last Run folder. In the right pane, second line down says Map Drive. Right click > Modify
- A box will open with “P” in it. Change to that next available drive letter that Windows is automatically mapping to, making sure it is in Caps. Click ok.
- Go back to the left pane. Click the “+” next to Last Run folder and you will see a folder named “A”.
- Left click the “A” folder. In the right pane, second line down says Map Drive. Right click > Modify. A box will open with “P” in it. Change to that next available drive letter that Windows is automatically mapping to, making sure it is in Caps. Click ok.
- In the left pane, go back to the HKEY_CURRENT_USER and click on the “-“ and shrink it.
- Go to HKEY_LOCAL_MACHINE > Software > PC Dynamics > Safehouse16 > Last Run folder.
- Left click the Last Run folder. In the right pane, third line down says Map Drive. Right click > Modify. A box will open with “P” in it. Change to that next available drive letter that Windows is automatically mapping to, making sure it is in Caps. Click ok.
- Close the registry editor with the **X** in the upper right corner.

Integration with LDAP

The CyberAngel with Wi-Trac works seamlessly with LDAP. Our gina.dll file wraps around the primary Gina that is in the system. The primary Gina / WinLogon is what interfaces with LDAP to verify if what a user has typed is a correct username / password combination. What our gina.dll file is looking for is if a user has tried 3 times to enter a valid username / password combination. It is immaterial to The CyberAngel with Wi-Trac where Windows is going to look for that verification of password correctness. Windows comes back to us with a valid / invalid response, and that is what The CyberAngel with Wi-Trac responds to for action.

Protecting Applications with The CyberAngel® Secure Drive

Moving Outlook E-mail Folders to the Secure Drive

- Open the Secure Drive and create a new folder called “Outlook”.
- Open Microsoft Outlook and click on File, then Open, then Outlook Data File.
- Right click on the Outlook.pst file, and then left click on Properties.
- Right click on the Location path, (C:\Documents and Settings\.....\Microsoft\Outlook) and left click on Select All, then Right click on the highlighted area and left click on Copy.
- Close Microsoft Outlook.
- Open My Computer (or Windows Explorer) and paste the path into the Address line and hit enter. This will take you to the Outlook folders for that User.
- Using the center scroll bar, scroll down until the Secure Drive is visible in the left pane.
- Click and drag the Outlook.pst file(s) and the .dat file into the Outlook folder in the Secure Drive. Then delete these files from the old location on the C: drive (in the right pane).
- Open Outlook, which will ask you where the .pst file is now located. Point to the .pst file in the Secure Drive (P:\Outlook\Outlook.pst). You may have to close Outlook and re-open again.
- Upon completion, if you do not authenticate with the CyberAngel password, your e-mails will remain encrypted and not accessible.

Moving the My Documents Folder to the Secure Drive

- Create a folder in the Secure Drive (i.e. MyProtectedDocuments)
- Right click on the My Documents folder on the Desktop
- Left click on the “Properties” button
- Left click on the “Move” button
- Select the folder you created in the Secure Drive. After clicking OK or Apply, it will ask you if you want to move the contents of “My Documents” from the C: Drive to the Secure Drive. Select Yes, and it will move all files into the Secure Drive.

Note: This will also eliminate the need to change the default save location for other programs such as Word or Excel to protect those application documents.

Moving Microsoft Word to the Secure Drive

Select the Option item on the Microsoft® Word Tools Menu to display the Options property page, then select the File Location Tab. Modify the locations of your Document and AutoRecover directories to point to your CyberAngel® Secure Drive. The Document directory is the default location where Word will suggest you to save your new files. The AutoRecover directory is where Word will create temporary files while you are editing documents to help you recover in the event of a system crash. You might create a folder within your CyberAngel® Secure Drive called Word Files to store all new documents and then you would use the file path P:Word Files in the Document and AutoRecover directories.

Moving Microsoft Excel to the Secure Drive

Select the Option item on the Microsoft® Excel Tools Menu to display the Options property page, then select the General Tab. Modify the path in the Default File Location box to point to your CyberAngel® Secure Drive. All new Excel files will then be saved as default to the CyberAngel® Secure Drive. You might create a folder within your CyberAngel® Secure Drive called Excel Files to store all new documents and then you would use the file path P:Excel Files in the Default File Location box.

Installing the Cisco VPN in the Secure Drive

- When logged in properly and the Secure Drive available install the Cisco VPN client changing the installation path to P:\Program Files\Cisco Systems\VPN Client
- Start MSCONFIG and uncheck the VPN Client (if the cvpnd.exe doesn't start this will prevent the installer from running)
- Go to C:\Program Files and create a folder Cisco Systems with sub folder of Cisco VPN
- The full path to that folder should be C:\Program Files\Cisco Systems\Cisco VPN
- Copy the file cvpnd.exe from P:\Program Files\Cisco Systems\VPN Client to C:\Program Files\Cisco Systems\VPN Client
- Start REGEDIT -- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CVPND
- Change the EventMessageFile value to C:\Program Files\Cisco Systems\VPN Client\cvpnd.exe
- Change the ImagePath value to "C:\Program Files\Cisco Systems\VPN Client\cvpnd.exe" including the quotes
- Copy the folder C:\Documents and Settings\All Users\Start Menu\Programs\Cisco Systems VPN Client to P:\Program Files\ folder
- Set the attributes of C:\Documents and Settings\All Users\Start Menu\Programs\Cisco Systems VPN Client folder to hidden including subdirectories
- Reboot
- If The CyberAngel with Wi-Trac is not successfully logged into you will not be able to start the VPN Client but the Cisco VPN service will start (it should automatically start as a service) you will not see the Cisco VPN client in the programs listing.

Uninstalling on Microsoft XP

Running the Config.exe from the System32 Directory

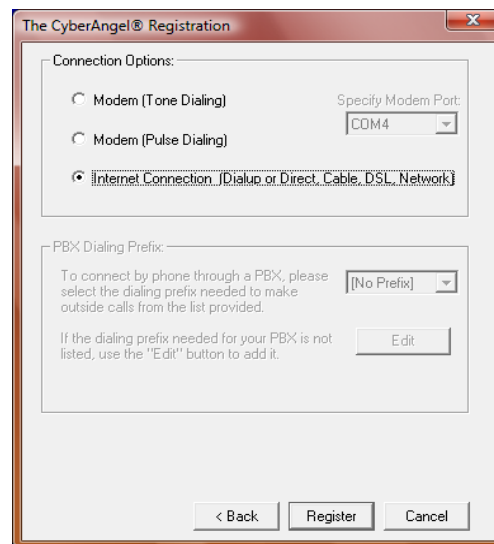
To perform the uninstall of The CyberAngel with Wi-Trac the Configuration Manager must be ran. The Configuration Manager can be located in the System32 folder as CONFIG.EXE. When you double-click on the CONFIG.EXE it will then prompt you for your CyberAngel password.



Once you authenticate correctly go to the "Uninstall" tab and choose continue. This will ask you how you are connecting to the Internet. Choose your connection and select connect.

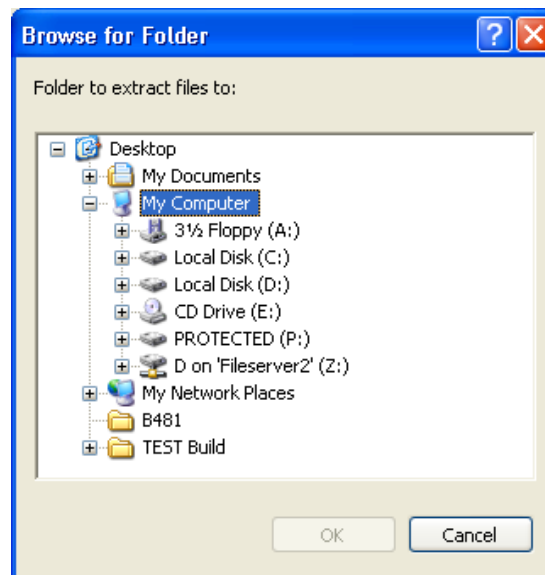
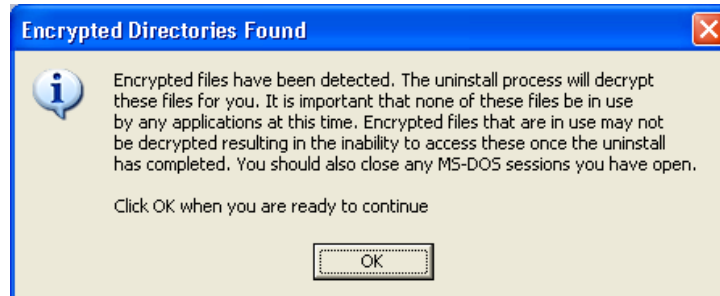
Connection to the CyberAngel Database

If the progress bar while connecting to the Monitoring Center stops at 20% for example, simply click cancel and try again. At that time the Monitoring Center is experiencing a high volume of traffic.

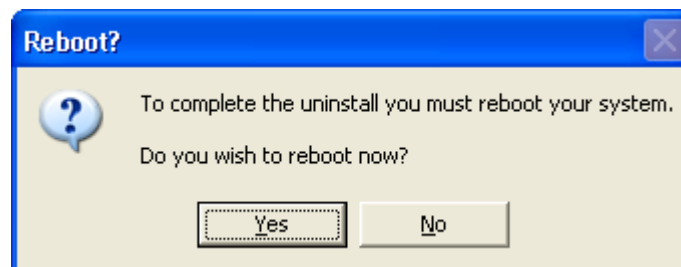


Decrypting Data & Files upon Uninstall

When you uninstall The CyberAngel with Wi-Trac , it will look to see if you have any encrypted files, and will prompt you to extract them to a location outside of the Protected Drive. A window will appear that will allow you to select a location to extract and decrypt those files. Depending on the size of the amount of files in your Protected Drive, it could take several minutes to extract and decrypt all of the files.



When the files are finished extracting, you will be prompted to reboot your computer. Click YES



Cleaning of residual files

The files that will reside on the computer after using the configuration manager and running uninstall are:

```
protected.sdsk = C:\Protected.Sdsk
mscae32.log = C:\mscae32.log
dsn1002.ca = C:\dsn1002.ca
sdwlib.dll = C:\WINDOWS\System32\sdwlib.dll
optic32.dll = C:\WINDOWS\System32\optic32.dll
sdwmap32.exe = C:\WINDOWS\System32\sdwmap32.exe
```

A simple right-click and delete will remove these files.

Uninstalling on Microsoft Vista

Right-Clicking the Config.exe from the System32 Directory

Vista requires you to right-click and “Run as Administrator” if you are not logged on already as the Administrator or Administrator Group, to successfully uninstall all the components of The CyberAngel with Wi-Trac.

Connection to the CyberAngel Database

If the progress bar while connecting to the CyberAngel Security Monitoring Center stops at 20% for example, simply click cancel and try again. At that time the CyberAngel Security Monitoring Center might be experiencing a high volume of traffic.

Cleaning of residual files

The files that will reside on the computer after using the configuration manager and running uninstall are:

```
protected.sdsk = C:\Protected.Sdsk
mscae32.log = C:\mscae32.log
dsn1002.ca = C:\dsn1002.ca
sdwlib.dll = C:\WINDOWS\System32\sdwlib.dll
optic32.dll = C:\WINDOWS\System32\optic32.dll
sdwmap32.exe = C:\WINDOWS\System32\sdwmap32.exe
```

A simple right-click and delete will remove these files.

Error Codes

User Interface error

The User Interface Error occurs when there is a problem either writing the msginaex.dll file to the System32 folder or changing the value within the Registry. If this occurs after an un-install, boot up in Safe-Mode and with in the Registry go to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon. Left-click on the Winlogon folder and the details will be displayed in the right hand side of the split-pane window. The name GINA with the value msginaex.dll will be displayed. Change the msginaex.dll to msgina.dll and reboot the machine.

NOTE: This only occurs on XP machines!

No “Protected” Drive

After the installation and the machine has come up from the initial reboot, the “Protected” drive should be created. If the “Protected” drive is not visible one must give permissions to the protected.sdsd file and the PC Dynamics folder in the Registry.

Identifying bad installs

A bad install can only be caught at the end of the registration. The CyberAngel User ID will have half a | and the end that is bold. To correct the problem, just reboot the machine and go to the configuration manager and uninstall and re-install The CyberAngel with Wi-Trac.

CyberAngel password prompt disappears

The CyberAngel with Wi-Trac password prompt may disappear due to security software such as; Spyware Blaster, Spybot, Trend Micro, Norton, etc. running on the machine and has performed a scan. Sometimes these programs tend to look at some of The CyberAngel with Wi-Trac files as a potential threat. To correct this problem have the software allow The CyberAngel with Wi-Trac files that it sees as a potential threat.

Installation without .NET Framework

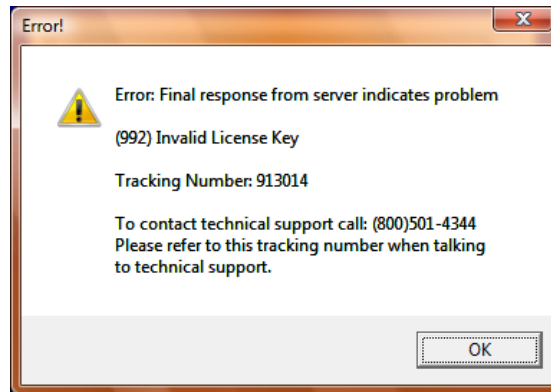
The .NET Framework is essential to The CyberAngel with Wi-Trac. These updates from Microsoft must be applied before the installation process.

No password prompt before uninstall

When The CyberAngel with Wi-Trac ‘s password prompt all of a sudden stops appearing after logging on, one will get the “Initialization Error”. This means that the drive containing the encrypted files is not accessible. The CyberAngel will have to be manually uninstalled at this point. Contact Technical Support **1-800-501-4344**.

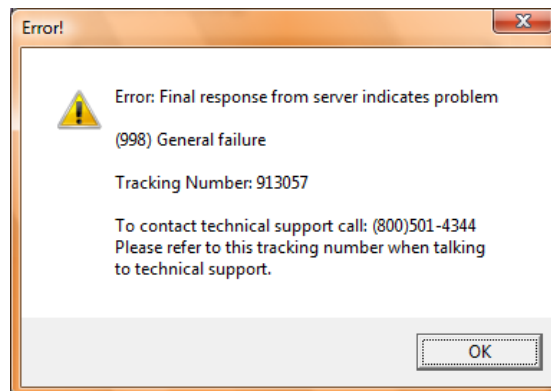
(992)Invalid License Key

This error occurs when one puts an invalid License Key in during the registration.



(998)General Failure Error

The (998) General Failure Error occurs when the License Key that you used is currently in use on another machine. Try another key or if this machine had hard drive problems and the CyberAngel was unable to be uninstalled, then contact Technical Support **1-800-501-4344** and someone will be able to free that license key.



Not running “Run as Administrator”

Vista requires users without Administrative privileges to use the “Run as Administrator” feature for applications and programs to load properly. Right-click the program icon you want to start, in the context menu that pops up will be an option called “Run as Administrator,” select this option and the program will run with Administrator privileges. This is to elevate the user to Admin privileges for any system changes or registry changes.

NOTE: The only time one should have to use the “Run as Administrator” feature is when opening the configuration manager.

No Credential Tiles

Vista doesn't have the usual logon screen as XP. Instead, Vista uses Credential Tiles. These are in a sense the same as the username on XP. Without a visible tile you cannot logon to that profile. After the installation of The CyberAngel with Wi-Trac and you come up to NO credential tiles then you must boot up in Safe-mode and check this path in the Registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers

You will need to delete the CyberAngel Credential provider # and replace it with the Microsoft Credential Provider #, then reboot the computer.

The Credential Providers are as follows:

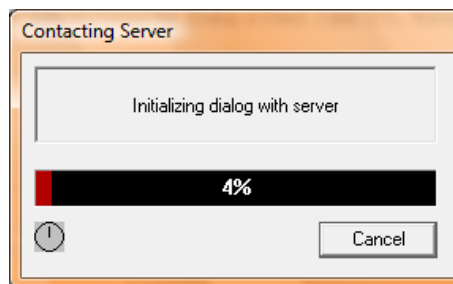
- A. Microsoft Credential Provider #: **6f45dc1e-5384-457a-bc13-2cd81b0d28ed**
- B. CyberAngel Wrapper Credential Provider #: **35A638D7-4CE7-43d2-9F9D-494B89E7FE31**

Registration Errors

During Registration the progress bar might stop at 4%. When this occurs simply click the Cancel button and click Register again. The reason for the progress bar to stop at this percentage is one of two things;

One, the firewall is currently blocking the packet from the monitoring server to the machine trying to register.

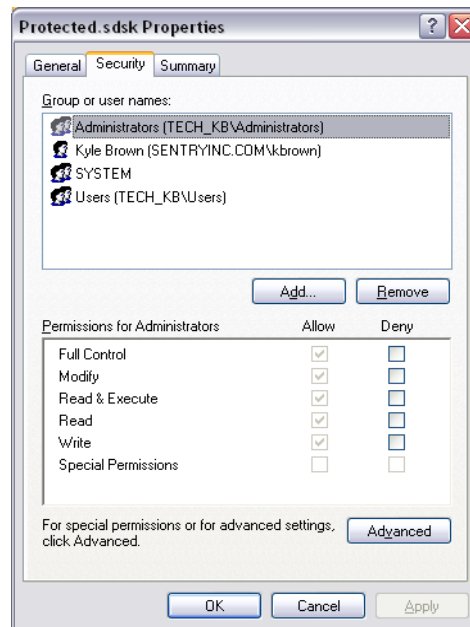
Two, we are experiencing a rather high volume of traffic at the time, so try again in a few minutes to register.



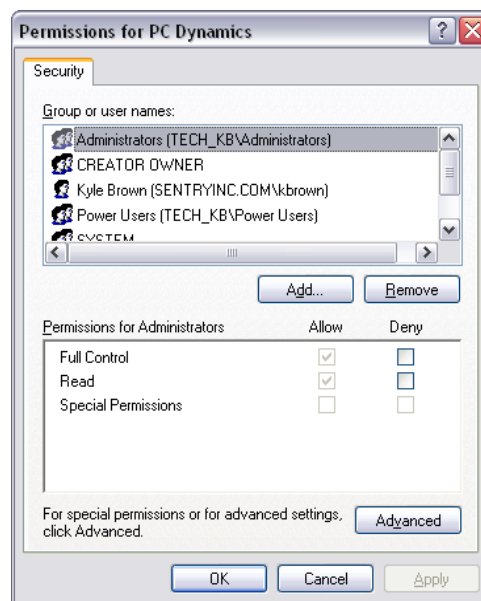
NOTE: Do not close or cancel your registration if you are getting this error message. Try again to connect a couple of times, waiting 2-3 minutes between attempts. If still unable to complete registration, please contact our Security Monitoring Center at 800-501-4344 for assistance.

Permission Issues

Certain permission issues can occur if the user is not part of the Administrator group. The way to keep The CyberAngel with Wi-Trac working for the non-Admin user is to give Admin permission rights to the protected.sdsk file.



Giving permissions to the Registry folder, PC Dynamics, will ensure proper working of The CyberAngel with Wi-Trac components.



Support Issues

Correcting the User Interface Error

Sometimes, usually due to packet loss, you can experience a “bad” installation. This will be exhibited by a gray error box stating that files cannot load when you are trying to reboot. Hitting “OK” will cause the computer to reboot and try to start again. You will need to go into Safe Mode to correct this.

- Boot into Safe Mode by pressing F8 during boot up process.
- Go to Start > Run > regedit.
- Go to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon
- Left-Click the Winlogon folder once and the details will be displayed in the right hand side of the split pane window
- Find the name "GINA" and double-click on this name
- Change the data value to "msgina.dll" from "msginaex.dll"
- Exit out of the Registry Editor and reboot the machine
- Once you log back into Windows you will need to uninstall the CyberAngel with Wi-Trac from the machine and then reinstall

Correcting an Aborted Installation

If you cancel an installation after you have started entering in registration information, there is a chance that residual files will be left on the computer preventing you from being able to go through the registration process again. You will need to make a change within the registry to allow you to proceed with a complete installation and registration.

- Go to Start > Run > regedit.
- Go to HKEY_LOCAL_MACHINE\Software\PC Dynamics.
- In the Left pane right click on the PC Dynamics folder and delete it.
- Close the Registry Editor window with the X in the upper right corner.
- Run wifisetup.exe again.

Forcibly Removing The CyberAngel with Wi-Trac

If you already have the CaSysMgr.exe program from a prior instance then proceed. If you do not already possess the CaSysMgr.exe program then please contact Technical Support at **1-800-501-4344** and someone will assist you in retrieving this program

- Run the CaSysMgr.exe program
- Click on Verification then "Installed Files"
- This will open another window within the System Manager that will show which files exist and their location.
- Check-mark all the files that say exist then right-click one of the checked files and choose "attempt to delete checked files". NOTE: 3-4 files might still remain. Don't worry we will delete them in the next few steps!
- Click on Modules/Services/Uninstall a Service
- This will open another window within the System Manager that will show all current Services installed on that machine and their current state
- There should be two Services running that are highlighted in blue. Check-mark these two Services and then right-click one of them and choose "uninstall all checked Services"
- Click on Modules\MsChkSys Installation\Registry Key Run Adjustment\Remove Registry Value. This will delete the **!Sysinit** out of the Run folder in the Registry
- Click on Process\Start\Regedit. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon and in the right side of the split pane window find the "GINA" name and double-click it. Edit the data value from "msginaex.dll" to "msgina.dll".
- Close the Registry Editor window with the X in upper right corner.
- While still in the System Manager click on Verification/Installed Files. Check-mark those few remaining files then right-click one of them and choose "Mark checked files for deletion"
- Reboot the machine
- Now you are ready to install the CyberAngel with Wi-Trac again

Removing the Windows Logon Screen

- Go to Start > Run > regedit.
- Go to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon
- In the Right pane find the AutoAdminLogon line and double click to open
- Setting the value at **1** instead of **0** will allow that computer to load directly to the desktop, bypassing the WinLogon and having The CyberAngel with Wi-Trac password box as the only authentication.

Code of Business Conduct and Ethics Policy

The trust and respect of our own employees, our customers, our strategic partners, our shareholders, opinion formers, other stakeholders and the general public – are assets that cannot be bought. This is why all CyberAngel Security Solutions, Inc. business must be conducted in adherence with high ethical and legal principles as the impact of wrongdoings and unethical behavior upon the Company could be substantial.

Corporate Policy

All business affairs of CyberAngel Security Solutions, Inc. (CSS, Inc.) are expected to be conducted in all respects in strict compliance with all applicable laws and regulations and in accordance with the highest standards of integrity and ethical behavior. All Directors, Officers, Employees, and Sales Consultants who represent the Company in the conduct of its affairs are expected to adhere to this Policy and avoid conduct or circumstances that might otherwise embarrass the Company. Everyone representing this Company has a duty to contribute to maintaining these standards by example and a heavier responsibility is borne by those who hold positions that more directly influence policy or practice as they must openly demonstrate leadership in applying ethical business practices.

One of our core values at CyberAngel Security Solutions is to strive for customer support excellence. We appreciate any feedback that you might have that will assist us in achieving this level of excellence. If you have a support issue of any kind, please let us know and allow us the opportunity to resolve the issue expediently and professionally.

CyberAngel Security Solutions, Inc.
475 Metroplex Drive
Suite 104
Nashville, TN 37211
Support@the cyberangel.com
1-800-501-4344

