Information Guide for Remote Security Suite

Backupanytime Ltd

The Remote Security Suite

The Backupanytime Remote Security Suite is your personal watchdog for your computer and its data.

If your computer is lost or stolen, you can log into your Backupanytime account from any computer using just a web browser. You will then be able to activate the Remote Security Suite to do any or all of the following:

- Erase **Sensitive Data** - You can order your computer to erase files on your computer that have been backed up to Backupanytime. You can even shred files with military-level file shredding technology that cannot be reversed. This prevents your sensitive data from falling into the wrong hands. Data will not be erased from the Backupanytime Data Centre.
- Take **Pictures & Record Sound** - The Remote Security Suite can activate your computer's built-in camera and microphone, recording in one minute segments and uploading to your Backupanytime account. This lets you see and hear who is using your computer.
- Send **Technical Details** - Your computer will collect and send to your Backupanytime account technical information about its environment, including networks to which it is connected and other data that might help zero in on who is using your computer.
- Track **a Stolen Computer** - Using a unique decollation technology that does not require a GPS in your computer, the Remote Security Suite collects and transmits location information. You can then look up this information in public databases to help find your computer.
- Freeze **Normal Backupanytime Operations** - This prevents a computer thief from accessing your Backupanytime account.

All the data collected by your computer will be transmitted and stored in your Backupanytime account, accessible with a web browser.

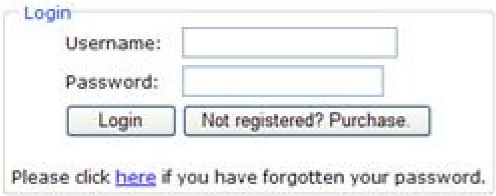
DISCLAIMER: The data collection features of the Security Suite rely on hardware installed on your computer, such as its camera, microphone, and wireless Ethernet card. Backupanytime will be able to collect information only if this equipment is installed, operational, and compatible with Backupanytime.

Relocation is approximate, and depends on the accuracy of the commercial databases Backupanytime uses to look up IP addresses and wireless SSID information. Backupanytime will not be able to exactly pinpoint the location of a missing computer with the accuracy of a GPS. The best it can do is to give an approximate location based on the IP address and the SSID broadcasts of wireless access points within range of its wireless Ethernet adapter.

Activating the Remote Security Suite

The Security Suite can be activated through a web browser by logging into your account at the Backupanytime website.

Browse to **http://www.backupanytime.com/login.htm** and select **Login** from the web site's menu.

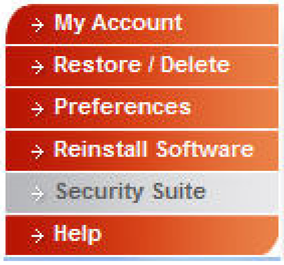


Please click here if you have forgotten your password.

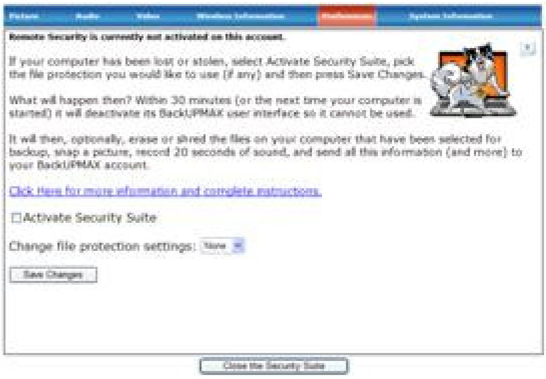
Enter your username and password. If you have forgotten your password, click the **here** link at the bottom of the login screen, and follow the instructions .

If you have forgotten your username, you must contact Backupanytime Tech Support during normal Tech Support hours. A fee may be charged for retrieving a username.

In an emergency, if you do not have access to a web browser, Backupanytime Tech Support may be able to activate the Remote Security Suite for you. There may be a fee charged for immediate access to a live Support Technician.



At the **User Console**, Click the **Security Suite** button.



Remote Security is currently not activated on this account.

If your computer has been lost or stolen, select Activate Security Suite, pick the file protection you would like to use (if any) and then press Save Changes.

What will happen then? Within 30 minutes (or the next time your computer is started) it will deactivate its BackUPMAX user interface so it cannot be used.

It will then, optionally, erase or shred the files on your computer that have been selected for backup, snap a picture, record 20 seconds of sound, and send all this information (and more) to your BackUPMAX account.

Click Here for more information and complete instructions.

☐ Activate Security Suite

Change file protection settings: None

To activate the Security Suite, place a checkmark in the **Activate Security Suite** checkbox.

Select the **File Protection** setting you want, or select **none**. **Selecting Erase or Shred WILL DELETE FILES FROM YOUR COMPUTER!**

Click **Save Changes** to activate.

Now What?

Within 30 minutes (or the next time your computer is connected to the Internet) it will deactivate its Backupanytime user interface so it cannot be used.

It will then optionally erase or shred the files on your computer that have been selected for backup, snap a picture, record 20 seconds of sound, and send all this information (and more) to your Backupanytime account.

The information is sent to your account over a secure connection, and is encrypted before transmission using the encryption key you selected when you installed Backupanytime.

Every 30 minutes that it is connected to the Internet your computer will transmit information from its wireless Ethernet card. This information may be able to be used to help locate your computer.

Your computer will continue to send information to your account as long as Backupanytime is installed on it (and the Remote Security Suite remains activated,) every time it is connected to the Internet.

Your account can hold 1 gigabyte of security information. When your account has collected 1 gigabyte, it will begin to delete the oldest information to make room for the latest.

Your 1 gigabyte of storage space allocated to the Remote Security Suite is separate from your normal disk storage quota, and is not a part of it.

How does Geolocation work?

Backupanytime collects several pieces of information that can point to an approximate location of your computer. Backupanytime gives you this information in a format that can help you look it up in various databases to help locate your computer.

A little detective work is usually required. Backupanytime will not be able to give you an exact address and room number. Geolocation may not work at all in sparsely populated areas. Databases may not be available for some areas.

IP Address – Every computer that is connected to the Internet has an IP address. This is number that is assigned to the computer when it connects to the Internet. Blocks of IP addresses are allocated by a central authority to various Internet Service Providers (ISPs) throughout the world. ISPs allocate specific addresses within their IP blocks to their customers as they log in and out of the Internet.

Backupanytime detects the IP address of your computer when it connects to the Internet. It then looks up your IP address in a commercial database that contains the geographical location of millions of IP addresses, and pinpoints its closest guess on a Google map.

Backupanytime’s guess about the location of a computer based on IP address alone is usually within a few miles of the true location. Most of the time, Backupanytime pinpoints the ISP itself, or his NOC or upstream provider. This is usually good enough to isolate a computer to a specific city or section of a city.

Wireless Networks - The landscape is full of wireless networks broadcasting important information. Your computer’s wireless Ethernet card can detect them, and Backupanytime can record them. Geolocation using wireless network information is not an exact science. It may require a little detective work and knowledge of the local area.

Think of a street-level map of your city. Many of the businesses along the streets have wireless networks installed. These wireless networks broadcast their signals in circles about 1000 feet around the wireless access points in the networks. Some signals are stronger, so the circles are bigger.

If your computer is at a McDonalds, it will pick up the McDonalds wireless signal the strongest. There’s also a Cigar Shop in the shopping centre behind the McDonalds, so your computer picks up that signal, too, but much weaker than the McDonalds. There’s a Hilton hotel ¼ mile away, and your computer can pick up that signal, too.

Backupanytime records all these signals and their strengths, and sends the data to your Backupanytime account. Now, if you could positively identify the signals, you could find the location of your computer like this:

The computer is very close to (maybe inside) a McDonalds. We know this because the signal is very strong. But we may not know which Starbuck's location. We also have a signal from the Cigar Shop, and a little farther away (because the signal is weaker,) a Hilton Hotel.

Now with a little detective work and local knowledge, we can find a McDonalds that is within ¼ mile of a Hilton hotel, and even closer to a Cigar Shop. Maybe we'll phone the Hilton and ask the location of the nearest McDonalds; or ask if there's a cigar shop nearby.

WIFI Geolocation Databases – Several companies and organizations are currently developing databases that contain the exact location of WIFI access points. This could be very useful in locating your lost computer.

Backupanytime is committed to improving our service to you. We will continue to improve our ability to pinpoint your lost computer using these databases as they grow.

War Driving Databases – "War Driving" is a game that involves collecting information about wireless networks. There are many variations of the game, some fairly innocent, and some illegal. They go something like this:

Players install software on their laptop computers or smart phones which detects and records information about wireless networks. They then drive their cars through neighborhoods and business areas recording networks and addresses as they go.

In the more innocent version of the game, players upload their records to a central database and get points for how many unique networks they detected. In other versions, players try to access the networks illegally.

Some of these War Driving databases are online and searchable. Since they are sometimes considered illegal in some locations, access to the databases via the web is sometimes unreliable.

The Backupanytime web site contains a list of these databases that can be used to look up wireless networks to try to find out where they are.

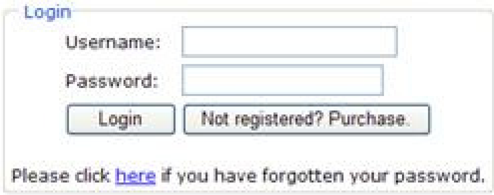
Viewing Security Suite Information

After you have activated the Remote Security Suite your computer will begin sending security information to your Backupanytime account. You can log into your account at the Backupanytime web site to view this information.

If you have selected to **Shred** or **Erase** files, those files will have been shredded or erased by the time the security information reaches your account.

⚠ **Your lost computer must be turned on and connected to the Internet for it to respond to your Activation request. In some cases, lost or stolen**

computers may never respond to Activation requests because they are destroyed or reformatted before they are connected to the Internet. It might take days or weeks for your computer to be turned on and connected.

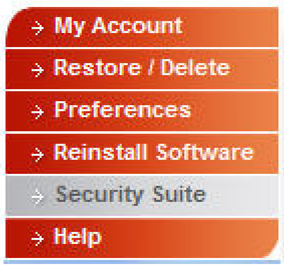

Login
Username:
Password:
Login
Not registered? Purchase.
Please click here if you have forgotten your password.

If your computer is turned on and connected to the Internet at the time you activate the Remote Security Suite, it can take up to 30 minutes for it to respond. If it is turned on and connected to the Internet after you activate it, it will respond immediately.

Browse to **http:// Backupanytime** and select **Login**

Enter your username and password. If you have forgotten your password, click the **here** link at the bottom of the login screen, and follow the instructions.

If you have forgotten your username, you must contact Backupanytime Tech Support during normal Tech Support hours. A fee may be charged for retrieving a username.

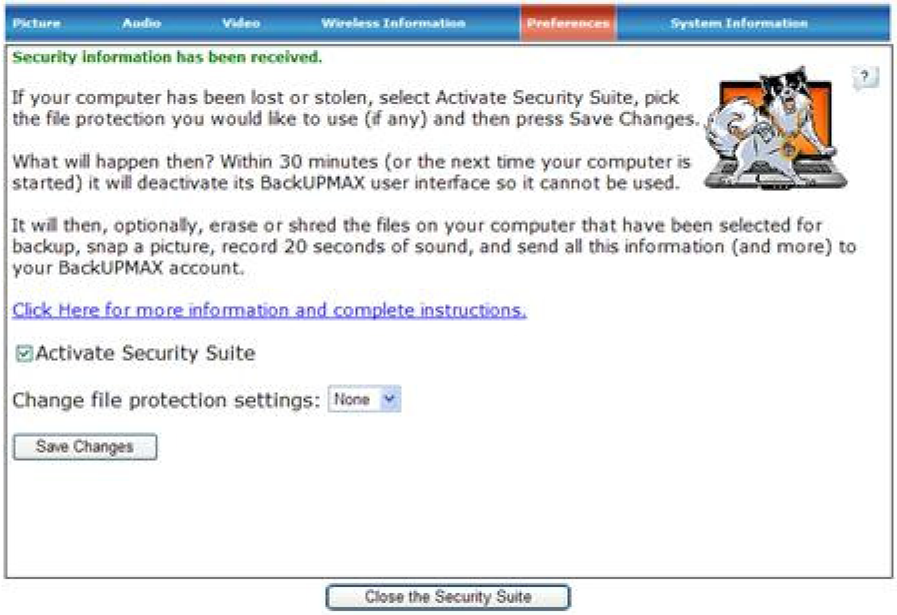


In an emergency, if you do not have access to a web browser, Backupanytime Tech Support may be able to activate the Remote Security Suite for you. There may be a fee charged for immediate access to a live Support Technician.

At the **User Console**, click the **Security Suite** button.

Check your account regularly to see if your computer has reported any information. When it has, you will be notified by a green message at the top of the page:

Security information has been received.



Security information has been received.

If your computer has been lost or stolen, select Activate Security Suite, pick the file protection you would like to use (if any) and then press Save Changes.

What will happen then? Within 30 minutes (or the next time your computer is started) it will deactivate its BackUPMAX user interface so it cannot be used.

It will then, optionally, erase or shred the files on your computer that have been selected for backup, snap a picture, record 20 seconds of sound, and send all this information (and more) to your BackUPMAX account.

Click Here for more information and complete instructions.

☑ Activate Security Suite

Change file protection settings: None

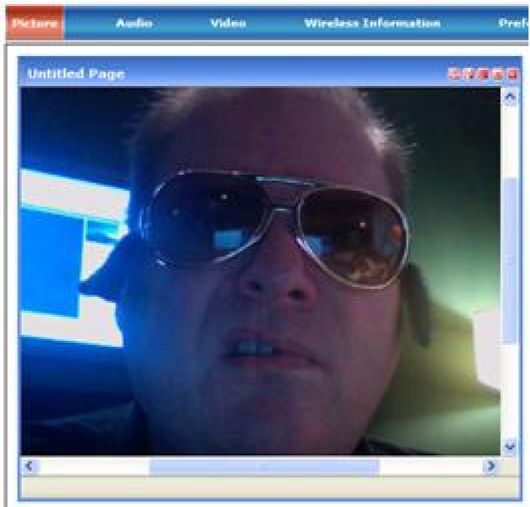
It can take as long as 30 minutes to receive all the information your computer might have for you. Usually, System Information, Wireless Information, still pictures and audio come in first, followed by Video.

Your computer sends still pictures, audio, and video every time Backupanytime is started. It sends wireless information every 30 minutes.

Some computers are not capable of sending Video. Some network cards are incompatible with the Security Suite. The information Backupanytime records for you are the best your computer is able to produce.

Still Pictures

Every time your computer snaps a picture, it is recorded in your Backupanytime account on the **Picture** tab, by date and time. Click the picture you want to view.



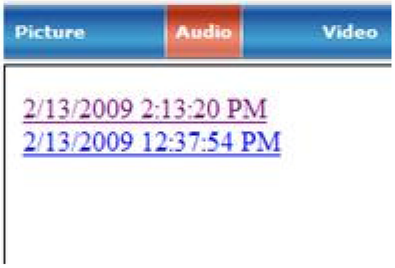
It looks like our stolen test computer was being used by Fake Elvis.

Look around the pictures to see if you recognize anything in the background.

Audio

If your computer supports Backupanytime Audio, you will get about 20 seconds of audio from your computer's built-in microphone every time Backupanytime is started.

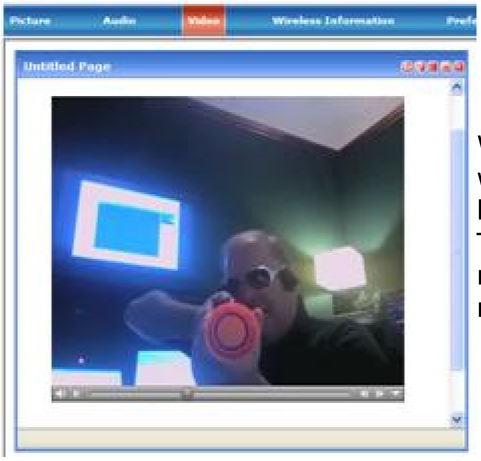
Click the date and time for the audio clip you want to hear. Try to recognize voices or background sounds.



2/13/2009 2:13:20 PM
2/13/2009 12:37:54 PM

Video

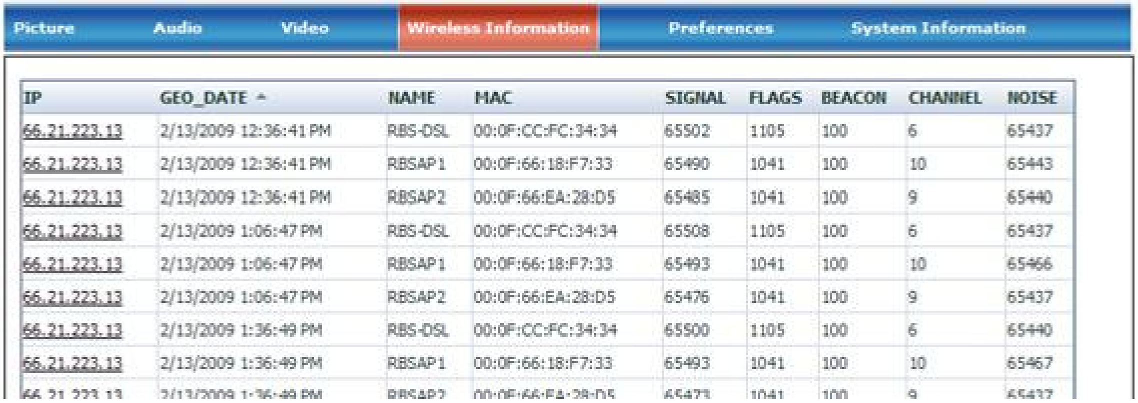
If your computer supports Backupanytime Video, you will get a 15 second video clip from your computer's built-in camera every time Backupanytime is started. You may also get audio with the clip, depending on your computer's capabilities.



We caught a video of Fake Elvis abusing our computer with a Nerf Gun. The background shows a room with a high ceiling, painted dark green, with wooden moldings. There's a big flat screen TV on the wall, and computer monitors behind F.E. – details that might help you recognize the location.

Wireless Information

Your computer sends information from its wireless Ethernet card when Backupanytime is started, and every 30 minutes thereafter.



IP	GEO_DATE ▲	NAME	MAC	SIGNAL	FLAGS	BEACON	CHANNEL	NOISE
66.21.223.13	2/13/2009 12:36:41 PM	RBS-DSL	00:0F:CC:FC:34:34	65502	1105	100	6	65437
66.21.223.13	2/13/2009 12:36:41 PM	RBSAP1	00:0F:66:18:F7:33	65490	1041	100	10	65443
66.21.223.13	2/13/2009 12:36:41 PM	RBSAP2	00:0F:66:EA:28:D5	65485	1041	100	9	65440
66.21.223.13	2/13/2009 1:06:47 PM	RBS-DSL	00:0F:CC:FC:34:34	65508	1105	100	6	65437
66.21.223.13	2/13/2009 1:06:47 PM	RBSAP1	00:0F:66:18:F7:33	65493	1041	100	10	65466
66.21.223.13	2/13/2009 1:06:47 PM	RBSAP2	00:0F:66:EA:28:D5	65476	1041	100	9	65437
66.21.223.13	2/13/2009 1:36:49 PM	RBS-DSL	00:0F:CC:FC:34:34	65500	1105	100	6	65440
66.21.223.13	2/13/2009 1:36:49 PM	RBSAP1	00:0F:66:18:F7:33	65493	1041	100	10	65467
66.21.223.13	2/13/2009 1:36:49 PM	RBSAP2	00:0F:66:EA:28:D5	65473	1041	100	9	65437

Wireless networks broadcast several kinds of information that can be useful.

NAME (SSID) – One of the things many (but not all) wireless networks broadcast is the Service Set Identifier, or SSID. This is a word or phrase (or numbers) that are used to identify the wireless network.

Many wireless networks broadcast an SSID that can be used to identify the owner of the network. For example, Hilton Hotels use "honors" (Hilton Honors Club) as their SSID.

✓ ***If your lost computer reports an IP address that services a Hilton hotel, and an SSID of a Hilton hotel, you can reasonably assume that your computer is in or near the Hilton hotel ssid, being used by someone who has access to the hotel's wireless network.***

SSIDs are not unique. They are assigned by the technician who installs the wireless network, and are often left at their default values. Default values for wireless access points are usually the name of their manufacturers, like "linksys" or "belkin54g."

Generic or default SSIDs are of little use in tracking a lost computer. What we're looking for are descriptive names like "McDonalds4503" and "cigarshop."

Mac Address – Every wireless access point has a unique Media Access Control (MAC) Address. Unlike the SSID, no two wireless networks broadcast the same MAC Address.

Signal – This is an indication of the relative strength of the signal being received by the computer from the wireless access point. It can be used in conjunction with other signals received at the same time to estimate the position of the computer relative to the access points.

As an example, if two signals are received, one barely stronger than the other, the computer might be about half way between the two. The more signals the better. Three signals can be roughly triangulated to locate a computer.

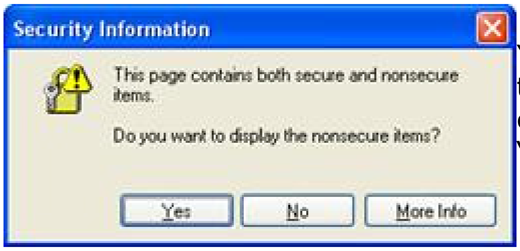
Noise – This is an indication of the amount of static, crosstalk, and noise in the Signal. It can be used to judge the reliability of a signal's strength.

Beakon – Wireless Access Points periodically broadcast their SSIDs and other information. On installation, technicians can set the Beakon Interval. This can be used to help further identify specific wireless access points.

Channel – Wireless Access Points broadcast on one of several channels. On installation, technicians can set the channel. This can be used to help further identify specific wireless access points.

Lookup by IP Address

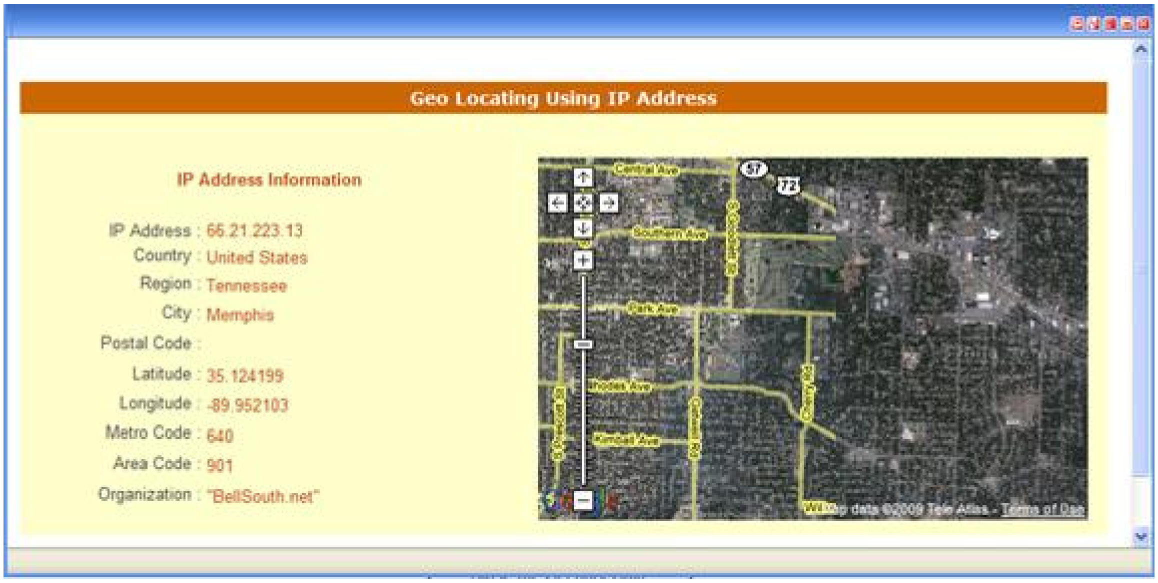
You can click on any of the IP Addresses in the **IP** column to display its location on a Google map.



This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Your computer might display this warning. It indicates that you are temporarily leaving the secure environment of the BackupAnytime website. Answer "**Yes**" to this warning to continue.



Geo Locating Using IP Address

IP Address Information

IP Address : 66.21.223.13
Country : United States
Region : Tennessee
City : Memphis
Postal Code :
Latitude : 35.124199
Longitude : -89.952103
Metro Code : 640
Area Code : 901
Organization : "BellSouth.net"

Backupanytime looks up your IP address in a commercial database that contains the geographical location of millions of IP addresses, and pinpoints its closest guess on a Google map.

Backupanytime's guess about the location of a computer based on IP address alone is usually within a few miles of the true location. Most of the time, Backupanytime pinpoints the ISP itself, or his NOC or upstream provider. This is usually good enough to isolate a computer to a specific city or section of a city.

Note: If the map does not display, it means that Backupanytime cannot locate the IP address.

File Protection

There are sensitive files on your computer – things you wouldn't want other people to have access to.

You may have accounting information, tax files, credit card numbers, bank account numbers, or trade secrets. If your computer belongs to your company, you may have very sensitive competitive information, customer lists, and other sensitive records.

If your computer becomes lost or stolen, you may be more concerned about the information on it falling into the wrong hands than you are about recovering the hardware itself.

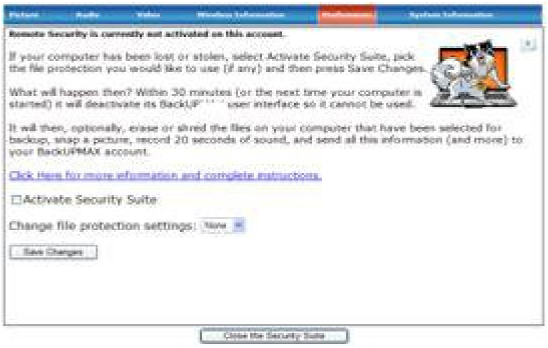
Backupanytime can remotely delete the files that you have currently selected for backup. It will not delete files from the Backupanytime Data Centres.

Backupanytime can help control the security of the files on your computer by erasing them two different ways.

Standard Erase – This is the fastest way for Backupanytime to erase files. It erases files just like the operating system does, except it does not move them into the Recycle bin (Windows) or the Trash (Mac). While this method is fast, it leaves "shadows" of the files behind, which in some cases can be recovered.

Shred – Shred is a special kind of file destruction that is used by the US military. Backupanytime uses the DoD 5220.22-M protocol to make files virtually unrecoverable using data forensics programs.

Select the type of file protection you want to apply, checkmark **Activate Security Suite**, and click the **Save Changes** button.



Remote Security is currently not activated on this account.

If your computer has been lost or stolen, select Activate Security Suite, pick the file protection you would like to use (if any) and then press Save Changes.

What will happen then? Within 30 minutes (or the next time your computer is started) it will deactivate its BackUP'' ' user interface so it cannot be used.

It will then, optionally, erase or shred the files on your computer that have been selected for backup, snap a picture, record 20 seconds of sound, and send all this information (and more) to your BackUPMAX account.

Click Here for more information and complete instructions.

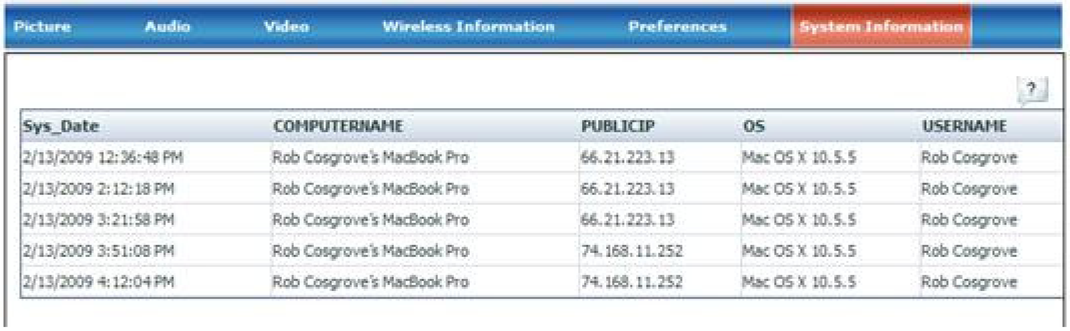
□ Activate Security Suite

Change file protection settings: None

System Information

The System Information tab contains information about your computer and its network. This information is sent by your computer every time Backupanytime starts, and every 30 minutes while it is connected to the Internet.

You can use this information to see if your hardware has been modified, view information about the networks it connects to, and as a "beacon" to tell when your computer is online.



Sys_Date	COMPUTERNAME	PUBLICIP	OS	USERNAME
2/13/2009 12:36:48 PM	Rob Cosgrove's MacBook Pro	66.21.223.13	Mac OS X 10.5.5	Rob Cosgrove
2/13/2009 2:12:18 PM	Rob Cosgrove's MacBook Pro	66.21.223.13	Mac OS X 10.5.5	Rob Cosgrove
2/13/2009 3:21:58 PM	Rob Cosgrove's MacBook Pro	66.21.223.13	Mac OS X 10.5.5	Rob Cosgrove
2/13/2009 3:51:08 PM	Rob Cosgrove's MacBook Pro	74.168.11.252	Mac OS X 10.5.5	Rob Cosgrove
2/13/2009 4:12:04 PM	Rob Cosgrove's MacBook Pro	74.168.11.252	Mac OS X 10.5.5	Rob Cosgrove