

# Phoenix FailSafe

## Frequently Asked Questions

### **Q. What is Phoenix FailSafe?**

A. Phoenix FailSafe is an overlay network infrastructure that allows a server to manage PC devices unobtrusively and securely over the internet. This enables device owners to protect and track lost or stolen devices, and to remotely provision and enforce usage policy on computing devices.

### **Q. What are the Phoenix FailSafe Components?**

A. Phoenix FailSafe consists of 4 discrete components or elements:

1. A Client Agent that resides on each PC device under management, whose job it is to maintain activity logs, and carry out instructions from the FailSafe server;
2. A server that maintains account information, policies, and settings associated with each individual PC device. This server is responsible for issuing commands or instructions over the internet to each client agent;
3. A Secure Communications Center (SCC) which provides a point-to-point communication channel between the FailSafe agent and server; and
4. A web client that allows the owner to monitor the location and status of PC devices.

### **Q. What Types of Location And Identification Data is Collected?**

A. Phoenix FailSafe captures the following types of tracking and identifying data:

1. GPS Activity. FailSafe will automatically detect the presence of a connected GPS device and periodically transmit GPS coordinates to the FailSafe server.
2. IP Trace. FailSafe captures the public and local IP addresses and identifies the ISP providing service.
3. Wi-Fi information. FailSafe not only identifies the public and private IP addresses, it also identifies Wi-Fi information such as the name of the wireless network, whether-or-not the network is secured (i.e., WEP enabled), and signal strength.
4. Caller ID. FailSafe has the ability to detect when a PC is connected to a phone line, and can initiate a stealth, toll free call to a monitoring center that can help identify the location of the PC via caller ID.
5. Webcam Photo's. FailSafe will automatically detect the presence of a connected webcam – whether built in or connected externally through a USB port, and take a candid picture from the webcam on startup that is sent back to the server. This can be very useful in identifying the perpetrator of a lost or stolen PC.
6. Forensic Tools. When a PC has been reported stolen, an owner can optionally enable a feature to have the FailSafe command center remotely download a keyboard logger to the stolen PC, and thereby capture forensic evidence about the perpetrator -- such as email addresses, user names, and other content the thief believes to be private. This can be combined with other location and identifying data to close the noose around the perpetrator of your stolen laptop.

**Q. How Does FailSafe Protect The Data On My PC?**

A. FailSafe has a number of features designed to protect the data on a monitored PC. As long as the PC is later connected to the internet, the following features are available:

Retrieve It: Allows the owner to remotely retrieve specific files on the lost or stolen PC. These files are all encrypted prior to retrieving them over the internet to the FailSafe server – and only the owner can access them.

Erase It: Allows the owner to remotely erase specific files and folders – using advanced deletion methods that have been endorsed by the United States Department of Defense (DoD)

Encrypt It: Allows the user to remotely encrypt specific files folders on a PC so that the files can be later retrieved when the device is recovered.

Disable It: FailSafe also allows an owner to remotely disable and re-enable a PC that has been lost or otherwise compromised.

**Q. How does Phoenix FailSafe transmit GPS information when there is no internet connection?**

A. The FailSafe agent maintains a series of logs that are stored on the monitored PC device. When the agent detects the presence of a GPS receiver, it first determines whether a GPS location fix can be established (based on simultaneous signals from 3 or more satellites). If it can establish a location fix, that information is stored in the form of GPS coordinates to a temporary log file. As long as the PC device is able to maintain a GPS location fix, it will continue to periodically log its location coordinates. When the PC later makes a connection to the internet, the location information associated with that device is immediately and securely transmitted to a FailSafe command center server, along with date and time information.

**Q. How does Phoenix FailSafe transmit Webcam photos when there is no internet connection?**

A. When enabled, FailSafe will automatically detect the presence of a connected webcam, and take a picture from the webcam on startup. That photo, along with date and timestamp information, is temporarily cached to a log file that sends the data back to the FailSafe server when an internet connection is established.

**Q. Does Phoenix secretly capture any personal information that I should be concerned about?**

A. No. Phoenix FailSafe does not transmit any personal information whatsoever, unless the PC owner explicitly enables a function to help track down a lost or stolen PC. Furthermore... the forensic information is encrypted and password-protected, so only the owner of the device can even read the forensic data captured – unless they choose to also share the password with local law enforcement.

**Q. Does Phoenix FailSafe potentially violate the privacy of the thief?**

A. One of the intended purposes of Phoenix FailSafe is to provide location and other identifying information to help recover a stolen PC device. While the privacy of the rightful PC owner is protected – and in fact further enhanced by FailSafe, the intent is to expose the identity and location of the thief so the PC can be quickly recovered. The lawful use of this product is no different than a property owner employing video surveillance techniques to track down and later prosecute a common thief. Let the thief beware that we mean business!

**Q. Does reporting a lost or stolen PC or filing a police report automatically enable all of the tracking and identification functions?**

A. No. By default, IP tracking is always enabled on the PC device. GPS may or may not be enabled by default – depending upon your PC manufacturer’s preference. Webcam and forensics are disabled by default, and are only employed when explicitly enabled by the device owner after a PC has been reported stolen.

**Q. Why would a user want to disable a PC versus immediately deleting the data?**

A. Disabling a PC can prevent its unlawful use, and can be executed immediately. Furthermore, a recovered PC can be unlocked without any impact to the underlying data. Also, IT may elect to implement safeguards that will cripple or otherwise disable a PC when used in a manner outside of an established set of parameters – such as trying to connect to the internet outside of the company’s secured network.

**Q. Why are there so many data deletion methods?**

A. The default delete function under most operating systems does not delete the actual files, but instead marks the spaces occupied by the subject file as free and updates the file system metadata structures, leaving the actual file contents intact on the physical medium. Secure file deletion programs work not only by unlinking a file but also by overwriting them with random data. This is intended to delete any remnants of the actual data that existed to prevent someone with the right forensic tools from recovering this deleted data. For very high security applications, overwriting the file several times is advised, and many government institutions have specific protocols for file deletion. While there is still some debate in regards to how many times a file should be overwritten to be considered secure, several passes is generally considered safe for most applications.