

# FAQ

## Computrace Products

TECHNOLOGY .....	1
COMPUTRACE AGENT .....	1
CUSTOMER CENTER.....	4
CONNECTIVITY.....	5
INSTALLATION.....	7
REGULATORY COMPLIANCE.....	7
OTHER TECHNOLOGY (encryption, cables, etc.).....	9

## TECHNOLOGY

### COMPUTRACE AGENT

#### **What is the Computrace® Agent?**

The Computrace Agent is the part of our technology that resides within your computer. It maintains contact with the Absolute Monitoring Center. In the event of theft, we can communicate with the Agent to determine the location of your computer, who has it, and what they're doing with it.

The Computrace Agent consists of two components:

Application Agent: Installed in the operating system (as a service) by running an installer. It makes regularly scheduled calls over the internet to the Absolute Monitoring Center and provides asset and location data on each Agent call. The Application Agent also manages the Absolute "helper applications" to support activities like data delete commands or to aid in theft recovery.

Persistence Module: Installed in the BIOS (or the firmware) of most laptops at the factory and activated during the Application Agent's first call to the Absolute Monitoring Center. It restores the Application Agent if it's removed. For example, if a thief steals a computer and reinstalls the operating system, the Persistence Module restores the Agent. The Persistence Module remains dormant until the Application Agent is installed.

#### **How does the Persistence Module become embedded into the BIOS firmware of a computer?**

Through our partnership with leading computer manufacturers, our Persistence Module is embedded in most computers during assembly at the factory.

#### **What is BIOS?**

BIOS = basic input/output system. Its primary function is to identify and initialize system component hardware (like video display cards, hard disks, etc.). Visit the BIOS [page](#) on Wikipedia for additional information.

# FAQ

## **On which computers is the Persistence Module embedded?**

Here is a current [list](#) of all computers that are manufactured with our Computrace Agent embedded in the BIOS firmware.

## **If my computer has the Computrace Agent embedded into the BIOS firmware, am I already protected?**

No. Even though our Persistence Module is built into the BIOS firmware of your computer, it is disabled and requires activation by installing the Application Agent.

To activate our Computrace Agent, you must purchase any of the Absolute Software products that include this technology.

Once the software is installed, the first call from our Agent to the Monitoring Center will detect and enable the persistence module. Once enabled, the self-healing feature of the persistence module in the BIOS will repair a Computrace Agent installation even if the hard drive is completely replaced.

## **I understand that the Computrace BIOS Persistence Module improves persistence. What is persistence and why is it of value to me?**

Persistence relates to the ability of our Computrace Agent to survive operating system re-installations, hard-drive reformat, hard drive replacements and hard drive re-imaging. This persistence is critical in order to survive unauthorized removal attempts in case of theft. The extra level of persistence provided by the Computrace BIOS Persistence Module enables the Absolute Theft Recovery Team to track and recover computers that have been stolen and provides customers with the ability to carry out commands such as data delete, device freeze, geolocation, and other remote security measures even if the hard drive has been tampered with or removed. The Computrace Persistence Module provides customers with the highest level of software-based computer theft recovery available on the market.

The persistence capability is strongest in laptops with the persistence module embedded in the BIOS firmware of the computer.

## **Are there different types of persistence?**

There are two levels of persistence for the Computrace Agent. The highest level occurs when the persistence module is embedded into the BIOS firmware of the computer. In this scenario, there is no additional hardware or software configuration needed for the Agent to be persistent. Computers that do not have the Computrace BIOS Persistence Module will have the software version of the persistence module installed in the partition gap on the hard drive.

## **What happens if I flash my BIOS? Will I need to reinstall the software?**

No. If the persistence module in the BIOS has been enabled, the self-healing capability will repair the Agent software and your computer will still be protected. The enable/disable state of the persistence module is stored in a part of the BIOS that cannot be flashed to remove it.

## **Will Computrace still work if I undergo an IMAC (install / move / add / change) process such as replacing a hard drive?**

Yes. The BIOS-resident self-healing capability will survive IMAC procedures such as imaging, hard drive replacement or operating system changes, and will continue to protect your computer.

# FAQ

## **What if my computer does not have the Persistence Module embedded in the BIOS firmware?**

You can easily install it in the partition gap on the hard drive of your computer. This allows the Application Agent to survive a standard operating system reinstall. However, unlike BIOS persistence, the Application Agent will not survive a hard drive swap.

## **Can the Computrace Agent be detected?**

The Computrace Agent is very difficult to detect. The software runs as a non-descript service, and is not listed as an application. Nor does the product show up on the programs menu listing or as a system tray icon.

## **How easily can the Computrace Agent be removed from my computer?**

Our Agent is one of the stealthiest and most tamper-resistant clients on the market. It is incredibly persistent and allows you to maintain a connection with each of your computers. If our Persistence Module was embedded in the BIOS firmware of your computer during assembly, our Agent can survive operating system re-installations, hard drive reformat and even hard drive replacements.

## **What if an unauthorized user still manages to delete the Computrace Agent?**

Our Agent employs a self-healing technology referred to as “persistence” that allows the Computrace BIOS-module (when the computer manufacturer embeds the Computrace Persistence Module into the BIOS or firmware of your computer) to essentially rebuild the Application Agent software even if the service is deleted. This self-healing feature can repair a Computrace installation in newly formatted and installed operating systems as well as freshly imaged systems.

## **What if I want to remove the Computrace Agent from my computer?**

If the Agent has been activated and you are an authorized user with the correct password, you can submit a request to have the Agent removed from your computer.

## **What is the footprint, or size, of the Computrace Application Agent?**

The Computrace Agent has a very small footprint, requiring less than 200Kb of disk space. It occupies a small amount of memory when idle, and when placing a call the Agent optimizes data transfer, which means a very low demand is placed on the network.

## **Will the Computrace Agent degrade our network, or clog it up?**

Computrace Agent communications require very little bandwidth and should have a negligible effect on your network traffic. A typical Agent call requires less than 200Kb of bandwidth.

## **How does the Computrace Agent communicate with the Absolute Monitoring Center?**

The Agent communicates with the Absolute Monitoring Center via the internet using reliable technology that is client-initiated, TCP-based, and always encrypted. Because the Agent initiates the connection to the Monitoring Center, it is inherently more secure than conventional auto-discovery mechanisms and does not rely on an open and listening port that could potentially render systems vulnerable to hackers.

## **What type of data is collected?**

The data collected allows you to manage the computers in your deployment as well as assists us in locating and recovering your computer in the event of loss or theft. Information is collected from the following categories:

- **Location:** Phone number, local IP address, routable IP address, MAC address, date, time.
- **User:** Electronic Serial Number (ESN), user name, computer name, and email address.

# FAQ

- **Hardware:** Basic system information: processor type, processor speed, hard disk size, hard disk space available, RAM size, computer make/model/serial number, number of CPUs, BIOS version (PC), BIOS date (PC), networking device description (PC).
- **Storage information:** Logical drive summary (drive name, type, file system, total size and available space), storage device (ATA, ATAPI/SCSI – e.g., hard drive, CD/DVD)(PC), floppy/removable drive, tape drive, RAM disk, network drive, other device, hard disk model, serial number, firmware revision (for SMART-enabled hard disks). Also, hard disk attributes for NT/2000/XP: raw read error rate, spin up time, start/stop count, reallocated sector count, seek error rate, power on hours count, spin retry count, calibration retry count, power cycle count.
- **Printer driver information:** Printer driver name, port, share name, server name.
- **Video system and monitor information:** Video device description and resolution, video display color depth, monitor type & manufacturer, and monitor refresh rate.
- **Modem information:** Modem model, port (if available), speed rating: maximum band rate (if available), networking device description. Mobile broadband adapter information includes physical location, user identification, equipment ID, subscriber ID, adapter phone number, and registered network.
- **Software:** Operating system, service packs for operating systems, software application, version, program & publisher; virus protection title & version, virus protection definition title & definition description.

## **Is the Computrace Agent monitoring my activities on the computer?**

No. The Agent is only collecting the data points described above for transmission to the Monitoring Center on the next scheduled call. Further action and data point collection occur only if the computer is reported stolen by you.

## **How do I manage updates and other work related to the Computrace Agent?**

Updates are easy. Once the client or Agent is installed, updates need only be done on the server side to enable various services. This allows other Absolute Software products and services to be turned on quickly and easily, without a cumbersome rollout of client software.

## **How often will my computer communicate with the Absolute Monitoring Center?**

Our “always on” Agent contacts the Monitoring Center once each day without any action from system users. If you report your computer lost or stolen, the Agent increases contact to every 15 minutes. In the event of a theft, we have Real Time Services that allow us to send an SMS message to initiate contact with the Agent in your computer versus waiting 24 hours for the next call. Read the Connectivity section of this FAQ for the detailed requirements for Real Time Services and Monitoring Center Initiated Calling.

## **CUSTOMER CENTER**

### **What is my Customer Center Account ID?**

Your Account ID is your unique identifier for your Customer Center Account. You will be asked for your account ID any time you contact the Absolute Global Support team. Your Account ID allows us to authenticate your status.

### **How do I find my Customer Center Account ID?**

1. Log in to [Customer Center](#) using your Username and password.
2. Your Account ID is displayed on the top right hand corner of the home page.

Your Account ID is confidential and should be safeguarded appropriately.

# FAQ

## How do I download my Customer Center account Agent files?

1. Log in to [Customer Center](#) using your Username and password.
2. Select **Administration**
3. Select **Accounts**
4. Select **Download Agent**

## I forgot my Customer Center password. What should I do?

You can retrieve your password on the [Forgot Password](#) page of Customer Center. You will be prompted to input your Username. Your password will be reset and emailed to you.

## How can I check how many licenses I have in my Customer Center account?

1. Log in to [Customer Center](#) using your Username and password.
2. Your license details are displayed on the home page in the Account Summary section.

## How do I check if a machine is calling in to my Customer Center account?

1. Log in to [Customer Center](#) using your Username and password.
2. Select **Reports**.
3. Select **Hardware Assets**.
4. Select **Asset Report**.
5. Select **And the field** from the drop down menu to filter your search.
6. Select **is or contains** as the data field.
7. Select **Show Results** to display the results.

## How do I request a data delete within Customer Center?

1. Log in to [Customer Center](#) using your Username and password.
2. Select **Data Delete**.
3. Select **Request Data Delete**.

## Where can I find more information and documentation about Customer Center and your products?

1. Log in to [Customer Center](#) using your Username and password.
2. Select **Documentation**.

## CONNECTIVITY

### How often will my computer communicate with the Absolute Monitoring Center?

Our "always on" Agent contacts the Monitoring Center once each day without any action from system users. If you report your computer lost or stolen, the Agent increases contact to every 15 minutes. In the event of a theft, we have Real Time Services that allow us to send an SMS message to initiate contact with the Agent in your computer versus waiting 24 hours for the next call.

### Am I able to communicate with a device immediately or must I wait for a scheduled Agent call?

Yes, you can communicate with a device immediately by forcing an Agent call. You may decide to do this if a device has gone missing or is exhibiting suspicious behavior.

Monitoring Center Initiated Calling (MCIC) uses real-time technology and provides for a faster connection than the

# FAQ

standard 24-hour period between Agent calls. A faster connection means that you can execute commands more quickly. For example, MCIC can be used to carry out data delete, Intel AT lock, and device freeze commands as soon as communication with the device is initiated. It also permits near real-time updates of the geolocation of the device (note that internet map locations will have a minimum delay of 30 minutes). This is advantageous since the first 24 hours post-theft or -loss is a crucial time.

The ability to use MCIC with Computrace products has the following prerequisites:

1. The computer must have a supported mobile broadband adapter (embedded or external).
2. The adapter or card must be activated with a plan from a telco service provider
3. The computer must be turned on
4. The adapter or card must be within the network coverage area and registered on the network
5. A phone number associated with the adapter must be known (either retrieved from the device using Computrace technology and posted within the Customer Center account, or known to the IT Administrator)

If the above conditions are met, MCIC technology can be used to initiate communication with a device. This capability supports Windows notebooks only.

## **How does MCIC work?**

MCIC is a customer initiated action. For enabled devices, MCIC is integrated into the Data Delete and Intel AT workflows. For expediting other commands or requests, MCIC can be accessed from the Device Summary page where you can select "Attempt Call".

Regardless of how you invoke the command, once selected, the following actions will occur:

1. SMS message transmitted
2. SMS message is delivered as soon as possible to the device, with receipt of successful delivery noted in Customer Center
3. Agent in device is woken, if no "free" connection is available, a high-speed cellular data connection is attempted
4. IP call (via cellular data connection or otherwise) occurs and command is executed

If the computer or cellular modem is off, or if the cellular modem is out of coverage, the *Call Now* message will be delivered as soon as the computer and modem are powered on and the cellular modem regains coverage.

## **What is a mobile broadband adapter and how do I know which devices in my deployment have one?**

Mobile broadband adapters can be embedded or externally connected to a computer. They provide an internet connection over a mobile network such as Verizon or AT&T. They also allow devices to send and receive SMS text messages.

A new report – Mobile Broadband Adapter Tracking (MBAT) – has been created within Customer Center so that you can track these expensive components within your asset base. Report attributes include physical location, user identification, equipment ID, subscriber ID, adapter phone number, registered network, etc.

## **Are there other advantages associated with real-time technology and Computrace?**

Yes, if you have Intel AT supported hardware, the Intel AT Lock Request feature can trigger an Intel AT lock using SMS messages with no Agent call required. The request to lock a device is sent from Customer Center to the device using SMS. The device responds with a SMS confirmation that it is about to lock. No internet connection is required!

# FAQ

To take advantage of this SMS-only immediate lock functionality, you will require Intel AT supported hardware ([view supported models](#)).

## **Can the Computrace Agent work through firewalls (including personal firewalls) to reach the internet?**

If you can browse, then Computrace will work. Our goal is as close to zero-configuration as possible. In some configurations, older versions of the Computrace Agent require the user to permit internet access the first time it attempts to contact the Monitoring Server. Newer versions of our Agent enhance the zero-configuration paradigm so that this first connection permission is not required.

## **Will the Computrace Agent work with a DSL or cable internet service?**

Yes. Computrace will work over a dial-up connection or with any internet connection (e.g., cable, DSL, wireless).

## INSTALLATION

### **Is the Computrace Agent easy to install?**

The Computrace Agent is very easy to install. The installer is a standard .exe executable. The Agent can also be easily installed on a corporate image or deployed using standard deployment tools such as Active Directory or logon scripts.

### **How do I install the Computrace Agent onto all of the computers in my deployment?**

You have many options. The Agent can be installed seamlessly on a corporate image or centrally deployed over a LAN. Once installed, the Agent simply needs an internet or phone connection to communicate with the Monitoring Center; no user intervention is required.

### **Are there other installation methods?**

You may also install the software through factory imaging processes from several PC manufacturers, through your own imaging process or through a network installation process. Absolute Software routinely provides tools, assistance and scripts in support of most mass-deployment technologies in use today. Contact your Absolute Software sales representative for more information.

## REGULATORY COMPLIANCE

### **How does the Computrace technology help with Sarbanes-Oxley compliance?**

It helps in two ways:

- 1) Section 1102 of Sarbanes-Oxley mandates stricter controls on financial data. Computrace technology can assist companies in placing stricter controls on access to financial data through auditing capabilities and tracking information on hardware and software. If a computer goes missing, our Data Delete feature allows IT administrators to remotely delete sensitive information and assess if confidential data has been accessed post-theft. The reporting functionality within the Absolute Customer Center will provide you with the proof you'll need to verify your compliance with government and corporate regulations.
- 2) Sarbanes-Oxley mandates that organizations report all company assets. Since IT assets are a significant portion of the total asset base of your organization, Computrace technology allows you to locate and report

# FAQ

on these assets – especially hard-to-track remote and mobile assets. All asset information collected by the Computrace Agent is stored, forming historical records and an accounting audit trail.

## **How do you help with compliance of State Data Breach Laws?**

State data breach laws mandate that organizations must report on any security breach that is reasonably thought to expose the personal information of any State residents. Computrace technology allows you to remotely delete data on missing laptops, reducing the risk of exposing this sensitive information.

Additionally, you can assess if confidential data has been accessed post-theft so you can know if a breach has occurred.

## **How do you help with FACTA and the Red Flag Rule?**

The Fair and Accurate Credit Transactions Act (FACTA) is intended primarily to help consumers fight the growing crime of identity theft. Accuracy, privacy, and limits on information sharing are included in FACTA.

The Red Flag Rule requires every U.S. service provider to develop, implement, and maintain a written comprehensive identity theft prevention program that specifically outlines the plans of the organization to protect customer information.

If a computer goes missing, our Data Delete feature allows Data Delete Administrators to remotely delete sensitive information and assess if confidential data has been accessed post-theft.

## **How do you help with the FACTA Disposal Rule?**

The FACTA Disposal Rule mandates the proper disposal or destruction of records containing private information. The rule applies to large and small organizations and to individuals who use consumer reports. Our Data Delete feature allows you to remotely delete sensitive data on computers nearing the end of their lifecycle. We use an algorithm that permanently deletes and overwrites the data, providing confirmation when the data delete is complete.

## **How do you help with Gramm-Leach-Bliley (GLB) compliance?**

Gramm-Leach-Bliley mandates that all companies protect the security and confidentiality of customers' private information. Under the provisions of Gramm-Leach-Bliley, personal information must be safeguarded at all times. Since businesses store personal information on remote and mobile computers, it is imperative to retrieve any lost or stolen device to ensure that the information contained on it was not used in a malicious manner. Computrace technology allows you to locate your IT devices at any time. Our Data Delete feature can help minimize risk of data exposure by remotely deleting sensitive files and assessing if confidential information was accessed post-theft. Additionally, our theft recovery software helps eradicate any security problems by identifying internal thieves.

## **How do you help with HIPAA compliance?**

HIPAA establishes rules for handling and securing medical records to ensure the privacy and security of patient information. Our technology helps organizations comply with HIPAA by deleting data from laptops that contain sensitive information, whether it's at end-of-lease or if a laptop turns up missing or stolen. HIPAA auditing requirements are also covered with our hardware and software tracking capabilities.

# FAQ

## OTHER TECHNOLOGY (encryption, cables, etc.)

### **I have encryption – why do I need to use Computrace technology?**

Encryption is a good start, but it does not address all aspects of data protection. The majority of data breaches are caused by insiders. In this scenario, encryption offers little protection as the employee will have access to the encryption keys and therefore the data. Our technology provides you with an audit log of exactly what data has been deleted. This allows you to verify that the sensitive data was removed from the stolen laptop which is imperative for regulatory compliance.

### **I have encryption software and the Computrace Agent in the BIOS. Will I have to worry about compatibility?**

No. Computers that have the Computrace Agent embedded in the firmware should have no compatibility issues with most encryption products.

### **With which encryption vendors is Computrace compatible?**

Computrace is fully compatible with all file-level encryption products. We've worked closely with Utimaco to ensure full compatibility with their SafeGuard Easy product and our technology. We are committed to continuing this work with all leading encryption vendors to ensure ongoing compatibility.

### **I have locks and cables – why do I need Computrace?**

Locks and cables are somewhat effective as a visible deterrent to theft, but in practice cables can very easily be ripped out of a secured laptop with nothing more than a good, strong tug. Cables provide no deterrent to the majority of laptop theft which is committed by internal employees who can easily obtain keys to cable locks. As well, locks and cables only work if the computer is at a desk which is not an option for mobile users.

### **I have asset tags – why do I need Computrace?**

Asset tags have proven to be an ineffective theft deterrent: The tag is simply removed by the thief after the computer is stolen.

### **I am considering radio frequency identification (RFID) – why do I need Computrace?**

RFID requires that the RFID asset tag be within close proximity to an RFID reader. These readers are expensive and require significant resources to implement. Also, once a laptop is removed from close proximity to a reader it cannot be tracked.