

# FAQ

## Computrace Products

PRODUCTS & FEATURES .....	1
PRODUCTS .....	1
FEATURE CATEGORIES .....	1
IT Asset Management .....	1
Data & Device Security .....	3
Geotechnology .....	11
Theft Recovery .....	13
Service Guarantee .....	14

## PRODUCTS & FEATURES

### PRODUCTS

	IT Asset Management	Data & Device Security	Geotechnology	Theft Recovery	Service Guarantee
Computrace Complete	●	●	●	●	●
Computrace Plus	●	●		●	
Computrace Mobile	●	●	●		
Absolute Track	●		●		
Computrace Data Protection	●	●	●		
Computrace for Netbooks	●	●		●	●

#### **Is there a consumer version of the Computrace products that I can purchase for my home computer?**

Yes. The same technology that protects deployments of computers within an organization is available with Computrace® LoJack® for Laptops by Absolute® Software for home use. Visit our [website](#) for more information.

### FEATURE CATEGORIES

#### IT Asset Management

##### **What is IT Asset Management and what does it mean to me?**

IT asset management is a strategy or plan that an organization implements so they can manage all of their electronic assets (computers, handheld devices, etc.). Management of these assets allows the company to keep track of where the devices are located and how they are being used.

# FAQ

It also provides for a centralized method of asset maintenance since it allows IT teams to know what type of software, hardware, or applications are loaded onto each machine and when these must be updated or removed. Devices cannot disappear due to asset drift if an organization is able to track them. And if the deployment includes leased equipment – each device can be located and wiped of data quickly so end-of-lease dates are not exceeded. Most IT asset management plans include a set protocol to follow in the event of theft or data breach to ensure the organization is compliant with government and corporate regulations. See the Regulatory Compliance section of this FAQ for more information.

## **How can Computrace products help me manage my IT assets?**

With Computrace products, you can manage all of your electronic assets with the ease of a single interface (regardless if a device is on or off your company network) within the Absolute Customer Center. You can monitor changes in asset information including user identification, physical location, and the installation of software/hardware that may not comply with government and corporate regulations. Most of our products provide you with advanced reporting capabilities. Computrace Plus provides you with basic reporting.

## **How is Computrace technology able to maintain regular contact with the devices in my deployment?**

The Computrace Agent resides within each computer in your deployment. It maintains contact with the Absolute Monitoring Center where it provides data from each device every day. You can analyze this data within your Absolute Customer Center account. The Agent calls in once each day. If you file a theft report, contact increases to every 15 minutes.

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

It depends on the device. In some instances you can use Monitoring Center Initiated Calling (MCIC) to force an Agent call. Scenarios where this could be helpful include if a device has gone missing or if it is exhibiting suspicious behavior.

## **What is Monitoring Center Initiated Calling?**

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

## **Are there prerequisites to use MCIC?**

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.

# FAQ

## 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 to device
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.

This provides you with important information so you can locate missing adapters and identify the users and computers associated with them.

## 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!

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

## Data & Device Security

### What is Data Delete?

Data Delete is a remote data deletion function that enables customers to delete sensitive data on target computers that have been stolen or lost. If your computer is stolen, you can set up a Data Delete request so that sensitive data on the computer is deleted the next time the computer calls in to the Monitoring Center. It can also be used for lifecycle management to ensure that computers are left clean and free of sensitive data at the end of their life or lease.

# FAQ

## What is Device Freeze?

Device Freeze allows you to manage devices remotely by freezing the device so that it is not functional and displaying a message to the end user explaining why the device is frozen and what they must do to unfreeze the device.

## How do I request a Data Delete or Device Freeze?

1. Log in to [Customer Center](#) using your Username and password
2. Go to the Data & Device Security section noted in the menu on the left hand side and select the appropriate action.

## Which Computrace products include Data & Device Security capabilities?

Data & Device Security capabilities are available with most Absolute Software products. Read the Products section of this FAQ for more information.

## Is pre-authorization required before I can use these capabilities?

Yes. Pre-authorization is required before this capability is available within your account.

## What does the pre-authorization process entail?

To begin, the signing officers from your organization must sign and return a pre-authorization agreement before the Data & Device Security capabilities can be enabled. The form is available in the Documentation section of the Absolute Customer Center. This agreement identifies the personnel authorized to perform Data & Device Security commands – known as “Security Administrators”, and your preferred authentication method. Upon receipt of the completed pre-authorization agreement, we will provide the Security Administrator(s) identified in your agreement with the ability to perform Data & Device Security commands within your Customer Center account.

## What are the authentication methods?

We offer two different methods:

- RSA SecurID tokens.
- Emailed authorization codes

You must specify which method you wish to use when you set up your Customer Center account and complete the pre-authorization agreement.

If RSA SecurID tokens are selected as the authentication method we will send the tokens to the Security Administrators identified in the agreement. Once received, Data & Device Security commands can be set up without any further involvement from us. Note that RSA SecurID tokens are an additional cost and must be purchased directly from Absolute Software.

## What is an RSA SecurID key/token and how does it work?

The RSA SecurID solution is the world’s leading two-factor user authentication system, relied on by thousands of organizations worldwide to protect valuable network resources. An RSA SecurID authenticator functions like an ATM card. Network and desktop users must identify themselves with two unique factors—something they know, and something they have—before they are granted access.

RSA SecurID authenticators are as simple to use as entering a password, but much more secure. Each end user is assigned a token which generates a new, unpredictable code every 60 seconds. The user combines this number with a password/PIN to log in to protected resources.

# FAQ

The RSA SecurID authenticator has a unique symmetric key that is combined with a powerful algorithm to generate each new time-based code. Only the RSA Authentication Manager knows which number is valid at any moment for any user/authenticator combination. Visit the [RSA website](#) for more details.

## **What is an authorization code and how does it work?**

An authorization code is a unique code sent to the e-mail address on file for the Security Administrator in response to a Data & Device Security command in Customer Center. The authorization code is valid for two hours after it has been issued, and can only be used for one operation. The authorization code may only be used by the Security Administrator who requests it. There is no charge for authorization codes.

## **Can I switch from RSA Secure ID® tokens to authorization codes or vice versa?**

Yes, but you can only choose one type of authentication method. Security Administrators may not use both methods at the same time. To switch authentication methods, contact Absolute [Global Support](#).

## **How do I request an authorization code?**

As a valid Security Administrator, you may request an authorization code as follows:

- In Customer Center, select **Data & Device Security**.
- Select **Request Data Delete Authorization Code**.
- You will receive your authorization code via email.

## **Is there an additional cost for any of the Data & Device Security capabilities?**

The only additional charge associated with Data & Device Security capabilities is for the RSA SecurID tokens. There is no charge to use authorization codes. For RSA SecurID tokens, a fee is charged for all tokens, including all renewals and replacements. You must purchase a separate token for each Security Administrator. Check with your Absolute sales representative for pricing.

## **How does Data Delete work?**

The Data Delete operation uses an algorithm that far exceeds the recommendations documented by the United States National Institute of Standards and Technology. For further details, see [NIST Special Publication 800-88: Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology](#). This document provides the specifications for wiping disk storage to guarantee that all data previously contained on the magnetic media is permanently erased.

When most computers delete a file, the computer does not actually remove the contents of the file but rather unlinks the file from the file directory system, leaving the contents of the file in the disk sectors. This data will remain there until the operating system re-uses the same sectors when writing new data.

Until the old data is overwritten (which may take months or even longer) it can be recovered by programs that read disk sectors directly, such as forensic software. In addition, even if a sector is overwritten, the phenomenon of data remanence (the residual physical representation of data that has been in some way erased) can make deleted data forensically recoverable.

In order to be sure that a file has been deleted properly, it is necessary to overwrite the data sectors of that file. It is not sufficient to erase or format the drive, as there are numerous forensic tools available to recover "lost" data on disk drives. This specification requires that every single location on a magnetic media device be written to three individual times, first by writing a fixed value (0x00) once, then its complement value (0xff) once, and finally random values once.

# FAQ

Our Data Delete algorithm exceeds this standard by overwriting the data 7 times (rather than 3) and by performing additional operations. The algorithm:

1. Can be set at your discretion to overwrite the target area 1, 3, or 7 times. Multiple overwrites will include an alternating pattern of 1s and 0s and the final write with a random value
2. Writes random data to the file
3. Changes the file attributes to "directory"
4. Changes file date/time stamp to a fixed value
5. Sets the file size to "0"
6. Changes the file name to a randomly-generated file name
7. Removes the new file name from the directory

## **Can the data be recovered from fixed disks/magnetic media once it has been deleted?**

No. The data is not recoverable.

## **Does Data Delete adhere to the US Department of Defense 5220.22-M Magnetic Media Sanitizing Standard?**

No. There are no software-only solutions that adhere to this standard as it requires physical destruction of the media by disintegrating, incinerating, pulverizing, shredding or melting the disk drive.

## **How can I prove that the Data Delete command was successful?**

The Data Delete process culminates in the creation of an audit log that verifies which files have been deleted. The audit log will be available within the Customer Center (Windows PCs only: Unless you are using a policy file and specify "no boot without log file" in the command).

## **When I run a Data Delete on a stolen computer, can I tell which files have been accessed post-theft?**

When you set up a Data Delete, you can choose to include the Created, Modified and Accessed Date in the log file (Windows PCs only). If this setting is enabled, the log file will display the date attributes beside the name of each deleted file. Including these attributes will increase the size of the log file.

NOTE: An Accessed Date for a file that is later than the date of theft does not necessarily indicate that the file has been compromised post-theft. Undetected malware, antivirus and spyware scans, automated backup and other similar applications may all trigger an Accessed Date change.

## **Do I have to delete the whole drive or can I choose specific files or directories?**

The Data Delete service is offered with 3 levels:

1. **Specific Files/Directories (PC Only):** Create a policy file identifying specific files, file-types and/or directories to be deleted. The computer will remain operational after the Data Delete process, assuming the user does not delete operating system directories or use a "no boot" option. For instance, you could choose to delete everything in the "My Documents" directory and all Word, Excel, PowerPoint and PDF documents, regardless of where they are on the drive.
2. **All Files except O/S:** All files excluding the operating system are removed from the hard drive. The computer will remain operational after the Data Delete process.
3. **All Files including O/S:** (Not applicable to Computrace Mobile devices) All non-OS files and some of the operating system files are removed from the hard drive. Once all non-OS files are deleted, Data Delete will begin a sector wipe starting at Sector 0. All user files (including programs and data) are deleted, and enough

# FAQ

of the OS files to stop the computer from booting. It is possible that some OS files will remain when the Data Delete terminates. The computer will not be operational when the Data Delete process completes.

In the case of a full deletion with OS, the Data Delete is a 2-phase operation – first all files except the OS are deleted, a log file is uploaded listing all the files deleted and then the OS deletion is launched. As the Computrace Agent will not be able to call once the OS deletion is in progress, the Data Delete is set to complete after the non-OS deletion is complete.

## **Will the Data Delete operation delete Windows XP and Windows Vista user profiles?**

Yes. Data Delete can delete all Windows XP user profiles by using an entry of “C:\Documents and Settings\”, or all Windows Vista user profiles by using a policy file entry of “C:\Users\”. Be sure to include the trailing backslash (“\”) at the end of the folder name.

## **What is a Data Delete policy file and how do I use it?**

A Data Delete policy file is a list of entries indicating specific files, file types and/or folders to be deleted. You can use a policy file to define the files you want to delete when you are invoking a data delete command. You can include the “no boot with log file” or “no boot without log file” options in a policy file if you want to delete files in a specific location first and then proceed with a full Data Delete. Policy files are supported on Windows computers only.

## **Can Data Delete remove locked files on Windows PCs?**

Yes. During the first deletion attempt, the Data Delete service will flag any locked files, such as an open Word document, to be moved to a safe location on the next reboot. Then, Data Delete will force a reboot to remove the file locks, and continue deleting the files after the reboot.

## **Can Data Delete remove locked files on Computrace Mobile Devices?**

No.

## **What safeguards are in place to ensure that only authorized users can launch Data Delete?**

Only those people identified as Security Administrators within the pre-authorization document are able to request this service. These Security Administrators must use the authentication method required to carry out the command. Here is an overview of the restrictions in place:

- The Data Delete request screen will not be visible within your Customer Center account unless you have submitted a signed and fully completed pre-Authorization agreement.
- You must be an authorized Security Administrator as detailed in the Pre-Authorization agreement.
- You must have Administrator-level access to the Customer Center.
- You must use the appropriate authentication method (RSA SecurID key or authentication code). These are linked to each specific Customer Center user and are NOT interchangeable between different users in an account or between different accounts.
- The password you enter on the Data Delete request screen must match the password for the current logged-in Customer Center user.
- Your RSA SecurID token value (time dependent) – when entered on the Data Delete Request screen – must match that on the Absolute SecurID server for your specific Customer Center user profile.

If the above conditions are satisfied, Data Delete will be set to run for the selected computer the next time the Computrace Agent calls.

# FAQ

In addition to these safeguards, an email is sent to the signing officers on the pre-authorization agreement each time a Data Delete command is requested, launched and completed.

## **Can Absolute run Data Delete on my computers without my permission?**

No. We cannot run Data Delete as it requires components that only a customer would possess (RSA SecurID token, authorization code, login/password, etc.).

## **Can I evaluate Data Delete?**

Yes. Contact your Absolute sales representative to set this up.

## **Is my data protected if the thief never logs on to the internet?**

No. But in our experience, most stolen computers quickly find their way back onto the internet. This is usually why they are stolen. Once your computer connects to the internet, the Computrace Agent will contact the Absolute Monitoring Center and the command will be executed. Remember that Agent call frequency increases to every 15 minutes (versus 24 hours) once a computer is reported stolen.

## **If a thief reloads the operating system, why do we need Data Delete, since the data will be deleted anyway?**

Internal theft accounts for the majority of corporate laptop thefts. In such a scenario the user will know all the passwords and will not need to reinstall the operating system. So in cases of internal theft, Data Delete is the perfect solution.

In the case of external theft the thief will often re-install the operating system, with or without reformatting the hard drive. If the operating system is reinstalled without reformatting, the files that make up the operating system will be replaced. However, sensitive data files will not be fully removed, and are likely to be accessed through the standard file table, or by using many widely available forensic tools. Data Delete will remove these files, ensuring the data cannot be recovered.

Performing a Data Delete on a stolen computer also provides the customer with an audit of what files have been deleted. This verification is required to prove regulatory compliance.

If the operating system is reinstalled and the hard disk drive is reformatted, it is more difficult to access any remnants of the original data files on the computer, because the file table structure and the sector size on the hard drive may change. However, it will still be possible to do a sector wipe on the stolen computer.

## **How long does it take to perform a Data Delete on a Windows PC?**

The time it takes to perform a Data Delete varies according to a number of factors on the target computer:

- Number of files
- Number of files > 100 Kbytes
- HDD speed
- Processor speed
- Available RAM
- Presence of Anti-Virus software

It takes longer to delete files than a normal (operating system level) delete because of the thoroughness of the Data Deletion algorithm. On average, the deletion speed on a Windows XP computer with a Pentium M 1.8Ghz CPU and 504 Mb of RAM is approximately 100 MB/minute. A "typical" data delete can take anywhere from two minutes to several hours, depending on the type of computer and the volume of data to be deleted.

# FAQ

If you are concerned about the speed of your Data Delete transaction, we recommend creating a policy file that lists the most important files first.

## **Can a Data Delete be stopped?**

Once the Data Delete process has begun, it cannot be stopped. If a computer is rebooted during this time, the Data Delete process will continue where it left off. If Data Delete has been scheduled on a stolen computer, but hasn't yet been initiated, you can cancel the Data Delete command from within your Customer Center account.

## **Are hidden files also deleted from Windows PCs?**

Yes.

## **Can I purchase Data Delete as a single product?**

No – Data Delete is a technical feature available with select Absolute Software products.

## **Should Data Delete be used for Software Compliance tasks such as the removal of unauthorized software?**

This is not recommended. Data Delete has been designed for the removal of sensitive data on lost or stolen computers. Using it to delete applications such as limewire.exe may leave the machine in an unstable state, with application shortcuts and supporting DLLs left behind. Using Data Delete for compliance also draws attention to the application, reducing stealth capabilities and making the recovery application more apparent to end-users.

## **What does Device Freeze do and how does it work?**

Device Freeze allows you to freeze a device and display a message to the user.

Authorized Security Administrators can select a device to be frozen within your Customer Center account. The command includes selecting a custom message that will be displayed to the end user. Usually this message will explain why the device is frozen and what the end user must do to unfreeze it.

On the next Agent call, the command will be executed, the device will freeze, and a message will be displayed. The device can be remotely unfrozen at the discretion of the Security Administrator.

## **How will Device Freeze help me?**

Device Freeze is a tool to encourage behavior on the part of the end user. This could be a scenario where you want a laptop returned, or you need to get your hands on a device as part of an audit, or you simply want to validate who's using the computer as in the case of device drift. In these instances, an authorized Security Administrator can freeze the device and display a custom message explaining what's happening, contact information (if appropriate), and what the end user needs to do in order to unfreeze the device.

## **Which operating systems and devices will be supported for Device Freeze?**

All desktop and laptop devices will work with the exception of Mac computers. Supported operating systems include:

- Windows® 7™ (32 & 64-bit)
- Windows® Vista™ (32 and 64-bit)
- Windows® XP® (32-bit only)
- Windows® 2000
- Windows® Server 2008
- Windows® Server 2003

Device Freeze is not available for Computrace Mobile devices.

# FAQ

## How do I set up a Device Freeze command?

The first step is to create the customized message you would like to display. You can save your messages and create a library where you can re-use messages.

1. Log in to [Customer Center](#) using your Username and password
2. In the Data & Device Security section, select **Create Device Freeze Message**
3. Create a name for your message. This will allow you to easily find the message within your library
4. Enter the message body in the field provided. Basic HTML formatting tags such as <b>, <i>, <font> are supported. You can preview the message and save it once it's complete

The second step is to select the device you want to freeze.

1. Log in to [Customer Center](#) using your Username and password
2. In the Data & Device Security section, select **Request Device Freeze**
3. Select the device
4. Select a message. The content will be displayed so you can ensure it is the desired message
5. Submit the request
6. On the next Agent call, the command will be executed and Agent call frequency will increase from every 24 hours to every 15 minutes

## Are there parameters for creating a message?

Yes, as follows:

- Message content may not exceed 4,000 characters.
- Content may include HTML, graphics, etc. URLs are not supported.
- Message content may be written and displayed in all currently supported languages

## What limitations exist with a Device Freeze command?

Devices with a theft report filed cannot be frozen. Devices that are frozen cannot have a theft report filed or a data delete command invoked.

## How do I unfreeze a device?

There are two different methods to unfreeze a device:

Via Customer Center:

1. In Customer Center, the device ESN is flagged to be unfrozen by the Security Administrator
2. On the next Agent call, the device will unfreeze and the message will no longer appear
3. The Agent call back frequency is re-set to occur every 24.5 hours

Via the device:

1. In Customer Center, the Security Administrator retrieves an unfreeze code for the device and provides this to the end-user
2. The end user is instructed to press ESC and enter the unfreeze code. The code is numeric only. Note that this is a blind entry with the end user typing the code without an entry screen.
3. The device will unfreeze and the message will no longer appear
4. On the next Agent call, call-back frequency is re-set to occur every 24.5 hours

# FAQ

## What is the end-user experience when a device is frozen?

The device will display and act in the following manner:

- Full-screen message will be displayed
- End-user **will not be able** to minimize or close the full screen message window
- End-user **will not be able** to open any new applications
- End-user **can** use the ALT-TAB command to scroll through any open windows and save any open documents
- End-user **can** reboot into Windows 'Safe Mode' but the freeze will remain
- End-user **can** reboot into Windows 'Safe Mode with Command-Line Only' and the freeze will NOT appear, but this does not provide a significant work-around since an end-user typically cannot accomplish much at the command line level
- End-user **can** remove and 'slave' the hard drive into another device and access the data on that hard drive

## Geotechnology

Geotechnology is one of our fastest growing feature categories. Geotechnology allows our customers to incorporate the physical location of a device into their IT Asset Management strategy. We currently provide geolocation and geofencing options within Customer Center, available with many of our Computrace products.

### What is geolocation tracking?

Geolocation tracking allows you to determine the physical location of your computers and mobile phones. You can see the location of each device on an internet map within your Customer Center account.

Detailed location information including latitude and longitude coordinates is available within the Device Location and Device Location History reports.

### What type of technology is required to geographically locate my IT assets?

GPS or Wi-Fi technology allows you to track your assets on an internet map. You will be able to see current and historical locations within about 33 feet. The use of GPS technology requires a GPS receiver. Visit the [Geolocation Technologies & Devices](#) web page for more information.

### What measures are in place to enhance the accuracy of the geolocation results generated by Wi-Fi networks?

There are two types of Wi-Fi networks: infrastructure and ad-hoc. Infrastructure networks use routers that are wired into a network similar to Wi-Fi routers used in offices (static locations). Ad-hoc networks are created when people set up their computers to allow other people to share their network connection. Since most ad-hoc networks are being broadcast by laptop (mobile) users, it's likely the physical location of these networks will constantly be moving which can result in some outlier hits in your Device Location reports.

Computrace geotechnology looks for and removes hits on ad-hoc networks. This limits the number of unknown or strange locations that may appear in your Device Location reports within Customer Center.

### How do I enable geotechnology capabilities for my account?

Before geotechnology capabilities can be turned on, you must sign a geolocation waiver form. This is located within the Documentation section of your Customer Center account. Follow the instructions provided. Once the signed form is returned, the Absolute Global Support team will enable geotechnology for your account.

# FAQ

## What is geofencing?

Geofencing allows you to create predefined boundaries to contain the physical location of the devices in your deployment.



## How does it work?

Geofencing is based on the same technology as geolocation, using Wi-Fi and GPS to track the physical location of a device. With geofencing, you can define a set of boundaries and receive an alert if any of your devices move outside the area you've defined.

## Is it difficult to create geofences?

No, it is extremely easy. It involves two steps, one to create the geofence, and the other to create the rule or condition that will trigger the alert:

To create a geofence:

- Within the Absolute Customer Center, access **Administration** → **Geofences** → **Create and Edit Geofences**.
- Use the geofencing tool bar (see below) to build a shape around the area you wish to define. Save the geofence.



# FAQ

To create an alert:

- Within the Absolute Customer Center, access **Administration** → **Alerts** → **Create and Edit Alerts**.
- Specify the Condition Field as **Location**, then **Is Outside**, and then select your geofence, and a minimum time period.

If any of your devices cross a boundary line, you will receive an alert within Customer Center so you can investigate further and determine if any action is required.

## **Is it possible to edit a geofence once it's been created?**

Yes, you can edit a geofence:

- Go to **Administration** → **Geofences** → **View and Manage Geofences**.
- Click on the name of your geofence and then update as required.

## **May I select specific devices to be contained within a geofence or must all of my devices conform?**

Yes, you may select specific devices. This can be done when you create your alert where you can specify a group of devices versus your entire deployment.

## Theft Recovery

### **What do you mean by "Theft Recovery"?**

Exactly what it says – we will help to recover your computer if it is stolen. If this happens, the Absolute Theft Recovery Team will work with local police to locate it and return it to you.

### **How does this work?**

If your computer is stolen, contact us. The next time your computer connects to the internet it will silently switch to theft mode with Agent contact increasing from once per day to every 15 minutes. This increased contact will allow the Absolute Theft Recovery Team to forensically mine the computer using a variety of procedures including key captures, registry and file scanning, geolocation, and other investigative techniques to determine who has your computer and what they're doing with it.

Most importantly, we will use our technology to pinpoint the physical location of your computer and work closely with local law enforcement to recover it.

### **My computer has been stolen! What should I do?**

You must file a theft report as follows:

1. Log in to [Customer Center](#) using your Username and password.
2. Select Theft Reporting.
3. Select Make a New Theft Report.
4. Choose the machine that has been stolen and provide the following information:
  - How the computer was lost
  - The details of the police theft report that you've filed

### **What if my computer is lost?**

If your computer is lost, you can use the geolocation feature within Customer Center to locate the device.

# FAQ

## Service Guarantee

### **What is the service guarantee and how does it work?**

You will be eligible to receive up to \$1000 if we are unable to recover your computer or perform the data delete service. Some conditions apply. For more details view our [service agreement](#).