PC PhoneHome™

Tracks & Locates Missing Computers

Version 3.0

95/98/ME/NT/2000/XP

Brigadoon Software, Inc
143 Main Street
Nanuet, New York 10954
Tel: +1-845-624-0909 Fax: +1-845-624-0990
Website: www.brigadoonsoftware.com

INSTALLATION GUIDE FOR PC PhoneHome™

THEFT RECOVERY SOFTWARE

INTRODUCTION

This document will assist authorized users to track and locate computers protected with PC PhoneHome™ software. The proper installation and configuration of PC PhoneHome™ is critical to the recovery process.

OVERVIEW: HOW PC PHONEHOME™ WORKS

Every computer connected to the Internet has its own Internet address called an "IP Address." An IP Address is a set of four numbers separated by 3 decimals. (*i.e., 255.255.255.255*) Your ISP (Internet Service Provider) controls a group of IP Addresses that it, in turn, assigns to its customers.

Dynamic IP Addresses

Most people receive a "dynamic IP Address" when they dial up their ISP. A dynamic IP means that every time you connect to the Internet, your ISP "loans" you an IP address for the duration of that connection. The next time you connect to the Internet through that same ISP, you will receive a new IP Address.

Static IP Addresses

If you connect to the Internet via an ISDN, DSL, Cable, Satellite, T1, T3 or some other type of high-speed connection, you probably have a "Static IP Address." A static IP Address means that your ISP assigns you the same IP address every time you connect to the Internet. It does not mean you "own" the static IP Address (it's still controlled by your ISP); it means you have the right to its ongoing use.

ISP Logs

ISPs keep records of who uses what IP Address and at what time (if it's a dynamic IP Address), and to whom they assign a static IP Address. PC PhoneHome™ contains a stealth email application that sends your pre-configured recovery information via proprietary protocol to an email address of your choice (including web-based email).

Included in that email sent by PC PhoneHome™ is your ownership and contact information, as well as the IP Address from which that stealth email was sent. From that information, it is possible to trace the message back (via the IP Address) to the ISP that controls that IP Address and obtain location information for the lost computer. With this information, law enforcement can obtain the necessary warrant to recover your stolen computer.

INSTALLATION

This section covers proper installation and configuration. The examples used here are for the installation of PC PhoneHome™ for Windows 95/98/ME/NT/2000/XP.

IMPORTANT!

IN ORDER TO PROTECT YOUR PROPRIETARY DATA AND TO PROVIDE YOU WITH THE HIGHEST PROBABILITY OF RECOVERY OF YOUR COMPUTER SHOULD IT BE LOST OR STOLEN, WE RECOMMEND THAT YOU USE THE SECURITY PROTOCOLS LISTED IN THE APPENDIX OF THIS DOCUMENT.

Image1 PC PhoneHome™ Installer.

PC PhoneHome™ uses a Zip archive. To begin Installation double click the pcph_v3.0.zip file. This will extract the installer file called PC PhoneHome-V3.0.exe in the same folder.

Double Click on PC PhoneHome-V3.0.exe to begin installation.

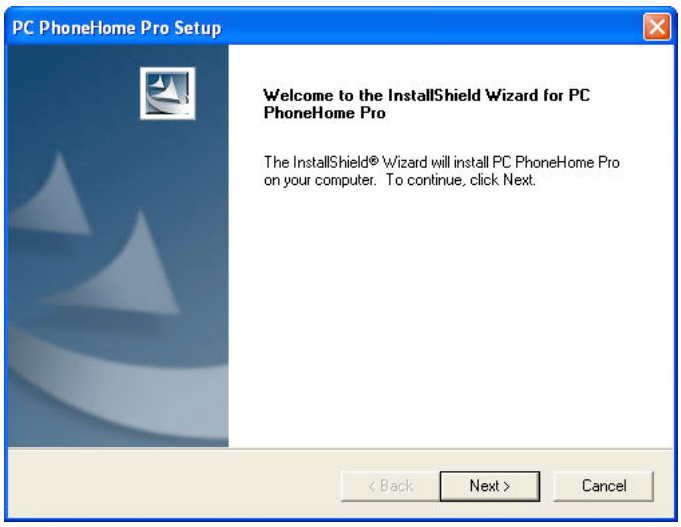


Image 2 Installation Setup

At the start of the install you will see this:

The PC PhoneHome™ install wizard is a menu-driven application. Simply follow the directions provided by the installer.

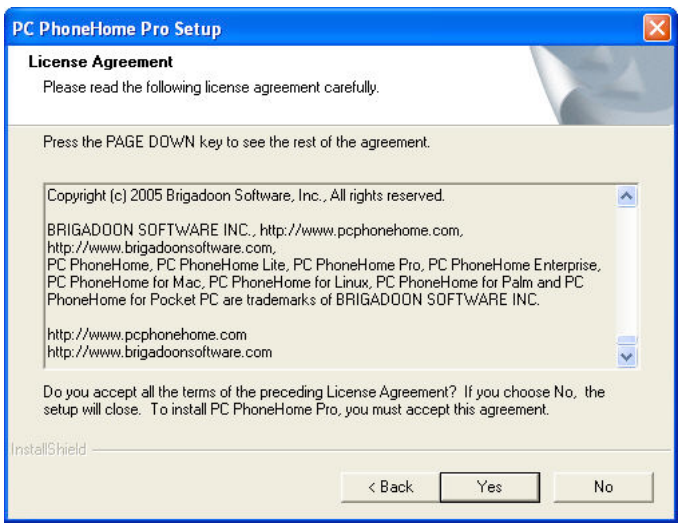


Image 3 License Agreement

The PC PhoneHome™ license agreement should be read in its entirety to insure that the registrant understands the legalities of using PC PhoneHome™ and agrees with the terms and conditions of using PC PhoneHome™ software.

IMPORTANT!!

The ownership information you provide in the configuration box for PC PhoneHome™ is the information that is sent to your designated email and to the Brigadoon Archives. It is also the same information you will turn over to the police in the event your computer is lost or stolen. It is important that you enter accurate and truthful information in the data field of the configuration window. The police will use this information as a basis to attain a court-ordered search warrant to retrieve your property. Less than accurate information may result in a search warrant application being denied.

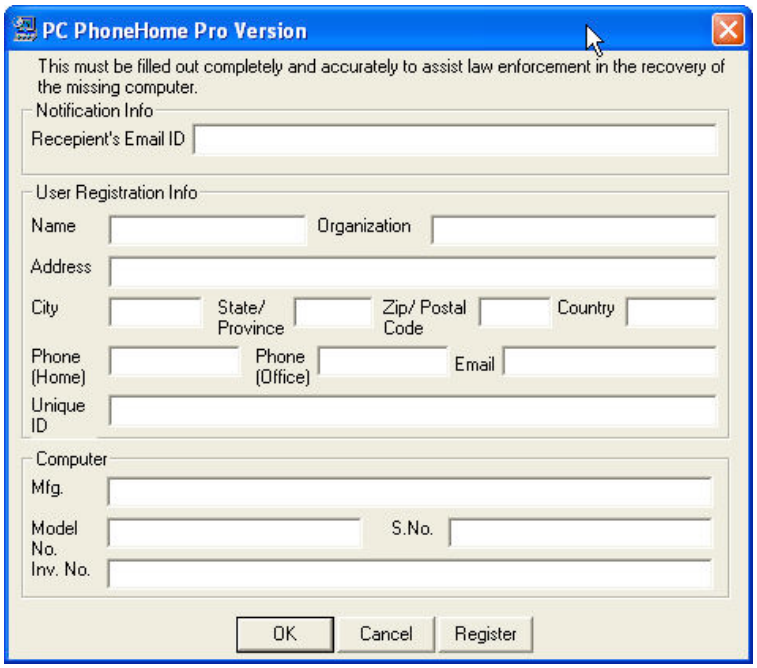


Image 4 PC PhoneHome™ Configuration Window

Notification Info

Recipient's E-Mail ID: Enter the E-Mail address to which you want your computer's location coordinates sent

Example: your--email-address@your-isp.com (web email addresses are OK too)

User Registration Info

Name: Your name

Organization: Your organization (if any-or else put in "None")

Address: Your address

City: Your City

State/Province: Your state or province

Zip/Postal Code: Your zip code or postal code

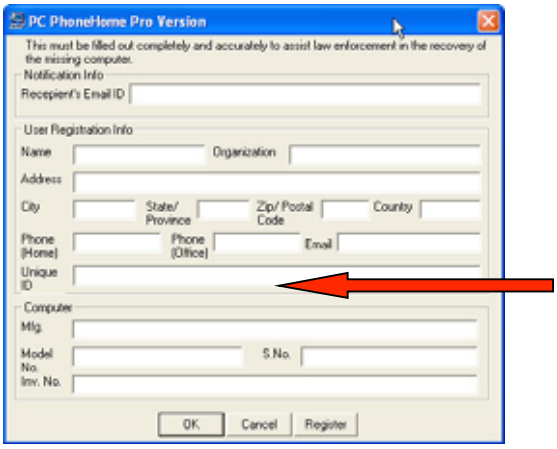
Country: Your country

Home Phone: Your home phone (for notification of recovery)

Office Phone: Your office phone, or another phone such as a fax or cell

Email: Your E-Mail: (for notification of recovery)

Unique ID: If you purchase a CD or download, you will get a Unique ID. Insert that Unique ID code here. (see right)



Computer Info

Manufacturer: What company made this computer?

Model Number: What model number is this computer?

Serial Number: What is the serial number on the back or bottom of this computer?

Inventory Number: What is the organization's inventory or asset tracking number of this computer? (or just put "none")

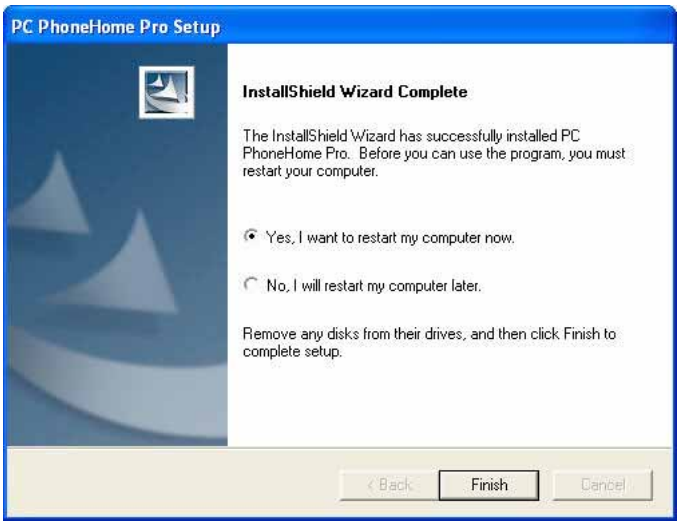


Image 5 Installation Complete

The PC PhoneHome™ installation is then complete. You will need to restart the computer to activate the software.

ONCE YOU COMPLETE YOUR CONFIGURATION AND REGISTRATION PROCEDURE (SEE THE SECTION ON "REGISTERING YOUR SOFTWARE"), REBOOT THE MACHINE. FROM THEN ON (PROVIDED YOU CONFIGURED YOUR APPLICATION PROPERLY) YOU NEED NOT DO ANYTHING MORE. PC PHONEHOME™ WILL SEND A STEALTH EMAIL TO THE EMAIL ADDRESS YOU ENTERED IN THE "RECIPIENT EMAIL" FIELD ONCE A DAY OR EVERYTIME THE PROGRAM SENSES YOU HAVE INTERNET CONNECTIVITY AND YOUR IP ADDRESS HAS CHANGED.

WHAT TO DO WITH YOUR INSTALLATION FILES

The beauty of PC PhoneHome™ is in its stealth: that is, you have a better chance of retrieving your lost or stolen computer if the person who has it doesn't know PC PhoneHome™ is on it and logs into the Internet, allowing PC PhoneHome™ to report it location through a stealth email. Therefore, any file left on the computer, such as "pcph_v3.0.zip" might tip off the thief that PC PhoneHome™ is on the computer. Therefore, we recommend that you keep a copy of the installation file OFF YOUR COMPUTER AND IN A SAFE PLACE AWAY FROM YOUR COMPUTER.

In addition, there is a pcph_v3.0 folder and a PC PhoneHome-V3.0.exe file that were created when you extracted the .sit during the installation process. We highly recommend you delete this folder and file off your computer as well. NOTE: Under the End User License Agreement, you are allowed to make an archive copy of PC PhoneHome™. We suggest that you keep a copy of pcph_v3.0.zip off your computer and archived.

NOTES

REGISTERING YOUR SOFTWARE

IMPORTANT! Even though you have a paid single user version of PC PhoneHome™, it is not fully operational until you register the software and receive a User Name and Serial Number.

Why? There is a legal basis for this: Remember, this application is primarily designed to track and locate missing and stolen computers. As such, the software is designed to (1) locate the computer; and (2) provide law enforcement the necessary tools they need to both (a) obtain a search warrant to recover the computer; and (b) prosecute the perpetrator.

Since, in most cases, PC PhoneHome™ was the PRIMARY instrument that provided the information used to find and prosecute a thief, the METHOD on how that instrumentality is used is subject to legal scrutiny.

The recovery process must withstand a defense's challenge on "can you prove that you used this software on your computer legally?" A good defense lawyer may challenge the software as being "illegally used" (i.e., bootlegged, or used in violation of the user license). He/she will challenge the prosecution to prove that it wasn't used illegally (proving a negative is always difficult).

But with PC PhoneHome™'s registration procedure, we can. Therefore, registration provides the basis for proving that the software is legally installed on the computer (remember, the license is for ONE computer for the length you own the computer).

30-Day Registration Period

The end-user is required to "Register" the software in order to continue to use it after the first 30 days. IF YOU DO NOT REGISTER YOUR SOFTWARE IN THE FIRST 30 DAYS AFTER INSTALLATION, IT WILL STOP SENDING LOCATION INFORMATION.

How do you register your paid single user version of PC PhoneHome™?

Auto-Registration

If you purchase PC PhoneHome™ from the Brigadoon Software website, you will receive an email containing files that allow you to automatically register PC PhoneHome™. It reads as follows:

REGISTRATION INSTRUCTIONS

Attached to this email, you should find a zip file containing the following Windows files:

"PCPHRegister.exe" and "[your Unique ID].phdt"

1. Unzip these files to a directory where you can find them (such as your desktop); and

2. Run "PCPHRegister.exe," then click on the "Register" button.

Upon clicking the "Register" button, you should have completed the registration process.

Manual Registration

If you purchased PC PhoneHome™ from another source, you will have to use the manual registration method.

You may request your Registration Codes by emailing your request, along with identifying information (i.e., such as your invoice number, and your name, address and Unique ID from the configuration screen when you installed PC PhoneHome™ to tech@pcphonehome.com.

Brigadoon Software will then check your Unique ID or electronic download invoice to determine if you are a bona fide licensee, and will then send your User Name and Serial Number and (if necessary) your Unique ID, usually by email.

Here is what the email will say:

Dear _____:

Here is your Registration Code along with install instructions.

Windows

Click on "Start"

Click on "Run" and then type "ConfigMod" in the field provided.

This should bring up the configuration window.

Enter the following in the Unique ID field:

Unique ID: [your Uninque ID]

Now click on the "Register" button in the bottom right corner and enter the following information:

Username: [your username]

Serial Number: [serial number]

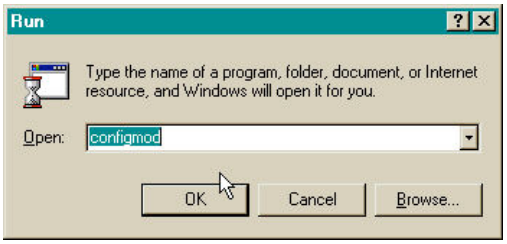
You should then get a box that says the Registration was successful.

Here's how you complete the manual registration process:

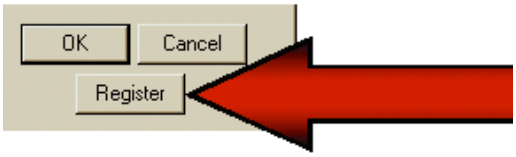
1. Click on "Start"

2. Click on "Run"

3. Then type "configmod" in the "Open" data field. This should bring up the configuration window.

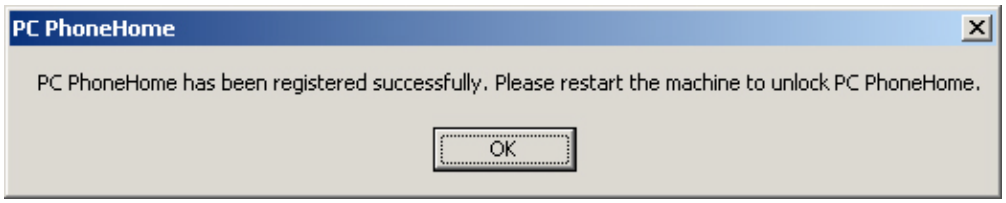


4. Click on the "Register" button on the configuration window



5. Enter your User Name and Serial Number (provided to you by Brigadoon Software) and then click "OK".

If you correctly completed the registration of your software license by correctly entering the User Name and Serial Number, you should then see the following window:



NOTES:

How MacPhoneHome™ Works

MacPhoneHome™ contains a stand-alone stealth email application that sends your pre-configured recovery information via proprietary protocol to the email address of your choice (including a web-based email address).

Every time the computer has Internet access, PC PhoneHome™ has the ability to send an identifying stealth email to the pre-configured Recipient's email address for location and recovery purposes. An example of how the message appears is as follows (color added for emphasis):

Sample of Received email including header

X-Persona: <BrigTech>
Return-Path: <sender@brigadoonsoftware.com>
Received: from mail.brigadoonsoftware.com (66.84.179.38)
by mail.mcf.com
with SMTP (Eudora Internet Mail Server 3.1b1);
Thu, 18 Oct 2001 11:10:21 -0400
From: sender@brigadoonsoftware.com
To: tech@brigadoonsoftware.com
Subject: Information
Date: Thu, 18 Oct 2001 11:10:21 -0400
Message-ID: 1208704675-101666554@mail.mcf.com

PCPH Pro For Win 95/98/ME/NT/2K

Date: 10-18-2001
Time: 11:10:21
Computer Name: SPARKY3223
User Name: Sparky3223
IPAddress : 66.84.179.38
Mac Address: 44-45-53-54-61-6F
Mac Address: 44-45-53-54-61-70
Mac Address: 00-80-C7-98-D6-9F
Serial Number: 392D12D8

Registrants Name: sammy
Organization: bsi
Address: 100 main st
City: nyc
State/Province: ny
Zip/Postal Code: 10002
Country: usa
Work Phone: 212-555-1234
Home Phone: 212-555-4321
E-mail: sparky@somewhere.com
Unique Identifier: my-unique-identifier-goes-here
Computer Manufacturer: ibm
Computer Model Number: 570
Computer Serial Number: 1231VF2937121-92
Inventory Number: bsi-34234

The information that is sent back to the monitoring email address provides two major bodies of information:

1. Information regarding ownership of the computer that is vital for its recovery (data in image 4 in blue); and

2. Information pertaining to the location identifiers in order to track the location of the computer at the time the computer was on the Internet and was able to send the stealth email message (data in image 4 in red).

The information included (data in image 4 in blue) above is vital in order to provide the court with probable cause so that the law enforcement agency in charge can obtain a search warrant necessary in order to recover the computer.

Section II - Recovering the Computer

During the normal course of monitoring, the owner and Brigadoon Software's redundant emergency backup system archive the information received from the computer in case there is a theft by saving the stealth email sent to the Recipient Email address by PC PhoneHome™.

Once a computer is reported as lost or stolen, report the incident to the applicable local law enforcement agency. Law enforcement should then generate a case number, and assign the case to an investigating officer. The investigating

officer will serve as the focal contact point in the recovery efforts. At that point, contact Brigadoon Software and provide as much information about the loss, including the case number and the contact information for the investigation officer. We will then provide you with recovery technical assistance at no extra cost.

Your PC "Phones Home"

The next time your lost or stolen computer has any kind of Internet access, it will send a new message. Once that new message is sent, a Brigadoon Software recovery technician can extract the IP address (the address on the Internet from which the message was sent) from the email and determine the Internet Service Provider that assigned that IP address.

Internet Service Providers log the telephone numbers (or, in the case of broadband service, the access point) of the incoming call BEFORE assigning an IP address. This telephone number or static access point is stored at the Internet Service Provider. This telephone number or access point provides the exact location of the missing computer. Internet Service Providers provide this telephone number or the access point information to the investigating law enforcement agency, which in turn uses this information to acquire a search warrant to retrieve the missing computer.

What is the "IP Address?"

In an IP network, each computer is allocated a unique IP address. The IP address is assigned to a computer once it makes a connection to a network. The Internet is composed of thousands of networks all connected together.

Each physical network has to have a unique Network Number, comprising some of the bits of the IP address. The rest of the bits are used as a Host Number to uniquely identify each computer on that network. The number of unique Network Numbers that can be assigned in the Internet is therefore much smaller than 4 billion, and it is very unlikely that all of the possible Host Numbers in each Network Number are fully assigned.

An address is divided into two parts: a network number and a host number. The idea is that all computers on one physical network will have the same network number - a bit like the street name, the rest of the address defines an individual computer - a bit like house numbers within a street. The size of the network and host parts depends on the class of the address, and is determined by address' network mask. The network mask is a binary mask with 1s in the network part of the address, and 0 in the host part.

Because IP addresses are a scarce resource, most Internet Service Providers (ISPs) will only allocate one address to a single customer. In majority of cases this address is assigned dynamically, so every time a client connects to the ISP a different address will be provided. Big companies can buy more addresses, but for small businesses and home users the cost of doing so is prohibitive. Because such users are given only one IP address, they can have only one computer connected to the Internet at one time. With an NAT gateway running on this single computer, it is possible to share that single address between multiple local computers and connect them all at the same time. The outside world is unaware of this division and thinks that only one computer is connected.

Client computers label all packets with unique "port numbers". Each IP packet starts with a header containing the source and destination addresses and port numbers:

Source address	Source port	Destination address	Destination port

This combination of numbers completely defines a single TCP/IP connection. The addresses specify the two machines at each end, and the two port numbers ensure that each connection between this pair of machines can be uniquely identified.

Each separate connection is originated from a unique source port number in the client, and all reply packets from the remote server for this connection contain the same number as their destination port, so that the client can relate them back to its correct connection.

Turnaround Time and Monitoring/Recovery

Once a message is received from a lost or stolen computer, it generally takes mere minutes to get enough information to either contact the ISP directly or provide law enforcement with the information necessary for them to contact the ISP and proceed with the inspection of the ISP's log records. From the ISP's log records, law enforcement obtains enough information to determine the exact address of the lost or stolen computer when it "Phoned Home."

TECH SUPPORT

If you need technical support or have any questions regarding your software, here is how you contact us:

Email (usually the fastest response): tech@pcphonehome.com

Fax: +1-845-624-0990

Telephone (during normal business hours-New York time): +1-845-624-0909.

APPENDIX: "HARDENING" YOUR HARDWARE

Disclaimer & Warning: While we recommend that you "harden" your computer to third party intrusion, the information provided in this Appendix **is advisory in nature only**.

All the hardening techniques of your computer's operating system rely on your Windows operating systems features. **THEREFORE, IF YOU HAVE ANY QUESTIONS, YOU SHOULD CONSULT MICROSOFT TECH SUPPORT DOCUMENTATION.**

Any actions involving computer firmware, such as changing your boot sequence in your computer's BIOS, is done so at your own risk. **IF YOU HAVE ANY QUESTIONS ABOUT YOUR COMPUTER'S BIOS OR FIRMWARE, YOU SHOULD CONSULT YOUR COMPUTER MANUFACTURER'S TECH SUPPORT DOCUMENTATION, OR (IN THE CASE OF YOUR BIOS SETTINGS) CONSULT YOUR BIOS MANUFACTURER'S TECH SUPPORT DOCUMENTATION.**

Introduction

To protect your proprietary data and to provide you with the highest probability of recovery of your computer should it be lost or stolen, we recommend that you take the following steps:

1. Set up different user accounts on your computer:
    a. For personal use: two accounts: Administrator and Guest (Managed);
    b. For organizations: three accounts: Administrator, Standard and Guest (Managed);
2. Password protect access to your Administrator and Standard accounts, but not your Guest account;
3. Have your computer boot directly into your Guest Account.
4. Utilize your computer's BIOS settings to change the boot sequence to prevent booting the computer from an external drive without authorization;
5. Use encryption software to protect your important data.

I. Accounts and users

Creating a User Account

You should not use your administrator account for everyday tasks on your computer. Your administrator account allows you to install software, but using it all the time is dangerous because viruses and Trojan horses accidentally run from the administrator account can cause greater harm to your computer. To prevent damage to your system, you should create a user account for every day use.

User Accounts overview

A user account defines the actions a user can perform in Windows. On a stand-alone computer or a computer that is a member of a workgroup, a user account establishes the privileges assigned to each user. On a computer that is part of a network domain, a user must be a member of at least one group. The permissions and rights granted to a group are assigned to its members.

User accounts on a computer that is a member of a network domain

You must be logged on as an administrator or a member of the Administrators group to use User Accounts in Control Panel.

User Accounts allows you to add users to your computer and to add users to a group In Windows, permissions and user rights usually are granted to groups. By adding a user to a group, you give the user all the permissions and user rights assigned to that group.

For instance, a member of the Users group can perform most of the tasks necessary to do his or her job, such as logging on to the computer, creating files and folders, running programs, and saving changes to files. However, only a member of the Administrators group can add users to groups, change user passwords, or modify most system settings.

User Accounts lets you create or change the password for local user accounts, which is useful when creating a new user account or if a user forgets a password. A local user account is an account created by this computer. If the computer is part of a network, you can add network user accounts to groups on your computer, and those users can use their network passwords to log on. You cannot change the password of a network user.

Note

- You cannot create groups using User Accounts. Use Local Users and Groups for that purpose.
- In User Accounts, you can place a user in only one group. Usually you can find a group with the combination of permissions needed by any user. If you need to add a user to more than one group, use Local Users and Groups.
- To improve the security of a password, it should contain at least two of these elements: uppercase letters, lowercase letters, and numbers. The more random the sequence of characters, the more secure the password.
- If you want to set up other password requirements such as minimum length, expiration time, or uniqueness, open Group Policy and go to Password Policy. For more information about changing password requirements, click Related Topics.

User Accounts on a computer that is a member of a workgroup or is a stand-alone computer

There are two types of user accounts available on your computer: computer administrator and limited. The guest account is available for users with no assigned account on the computer.

Computer administrator account

The computer administrator account is intended for someone who can make system-wide changes to the computer,

install programs, and access all files on the computer. Only a user with computer administrator account has full access to other user accounts on the computer. This user:

- Can create and delete user accounts on the computer.
- Can create account passwords for other user accounts on the computer.
- Can change other people's account names, pictures, passwords, and account types.
- Cannot change his or her own account type to a limited account type unless there is at least one other user with a computer administrator account type on the computer. This ensures that there is always at least one user with a computer administrator account on the computer.

Limited account

The limited account is intended for someone who should be prohibited from changing most computer settings and deleting important files. A user with a limited account:

- Cannot install software or hardware, but can access programs that have already been installed on the computer.
- Can change his or her account picture and can also create, change, or delete his or her password.
- Cannot change his or her account name or account type. A user with a computer administrator account must make these kinds of changes.

What Operating Systems We Support

Windows 95, 98 and ME are not secure systems by default. These operating systems were designed for home use where security was previously looked at as less important. A good example, if you create multiple user profiles on your computer running the old Windows 9x, you see the password dialog box (logon window) when you start Windows. This may suggest that the your computer is secure - it not! you can simply click Cancel or hit the Esc key and get complete access to all users files and folders.

We therefore only provide hardening recommendations for Windows NT, 2000 and XP.

Here is how your create user accounts for the currently supported Windows Operating Systems:

Windows XP

To create a user account in Windows XP:

1. Click the **Start** button in the lower left corner of the desktop.
2. Click **Settings**, then click **Control Panel**.
3. In the **Control Panel** window, click **User Accounts**.
4. In the **User Accounts** window, click **Create a new account**.
5. Enter the user account name in the **Account Name** field and click **Next**.
6. Select the **Limited** radio button, then click **Next**.
7. Click **Create Account**.
8. In the **User Accounts** window, click on the new account.
9. Click **Change the password**.
10. Enter the desired password (this should be different than the administrator password).
11. Verify the password and add a password hint.
12. Click **Change Password**.
13. Log out of the administrator account by hitting CTRL-ALT-DEL and selecting **Log Off**. Then log back in as the new user account.

Windows 2000

To create a user account in Windows 2000:

1 Click the Start button in the lower left corner of the desktop.
2 Click Settings, then click Control Panel.
3 In the Control Panel window, click Users and Passwords.
4 In the Users and Passwords window, select the Users must enter a name and password to use this computer check box.
5 Click Add.
6 Enter the User Name and Full Name, then click Next.
7 Enter the desired password (this should be different than the administrator password).
8 Click Next.
9 Select the Standard User radio button, then click Finish.
10 Click OK.
11 Log out of the administrator account by hitting CTRL-ALT-DEL and selecting Log Off. Then log back in as the new user account.

Windows NT

To create a user account in Windows NT:
1 Click the Start button in the lower left corner of the desktop.
2 Click Programs, then Administrative Tools (Common), and then User Management.
3 In the User Management window, click New User.
4 Enter the User Name and Full Name.
5 Enter the desired password (this should be different than the administrator password).
6 To allow the user to select a new, private password, select the User Must Change Password at Next Logon check box.
7 Click OK.
8 On the Start menu, click Shut Down, select the Close all programs and log on as a different user radio button, then click Yes.

II. Have your computer boot directly into your Guest (Managed) Account.

We recommend that you have your computer automatically log in to the Guest (Managed) account you created. From there you can log out and then log in to either your Administrative or Standard account, as needed. There a number of reference links to Microsoft's website with step-by-step instructions. They are:

Enabling Automatic Logon in Windows XP

You can configure Windows XP to automate the logon process if your computer is not part of a domain. Click "Start", click "Run", and type "control userpasswords2". Clear the "Users must enter a username and password to use this computer" check box. Click "Apply". Enter the user name and password with which you wish to automatically log on, and then click "OK". Click "OK" again and you're all done.

This feature allows other users to start your computer and use the account that you establish to automatically log on. Enabling auto logon makes your computer more convenient to use, but can pose a security risk.

For more information on "How to Enable Automatic Logon in Win XP" see:
http://www.support.microsoft.com/default.aspx?scid=kb;en-us;315231

Enabling Automatic Logon in Windows 2000

If you have a Windows 2000 Professional computer that is not part of a domain structure, you can enable automatic logons easily (without editing the Registry). Go to Control Panel, and open the "Users and Passwords" applet. Clear

the box next to "Users must enter a user name and password to use this computer check box." You may also have to click the “Advanced” tab, and clear the box next to "Require users to press Ctrl-Alt-Del before logging on."

Note that if the computer is a member of a domain, that these options may not be available. Also keep in mind that this is a potential security risk, since the computer will be available to anyone, even if they don't know the password.

For more information on “How to Enable Automatic Logon in Win 2000 Pro see:
http://www.support.microsoft.com/default.aspx?scid=kb;en-us;234562

Enabling Automatic Logon in Windows NT

Windows NT allows you to automate the logon process by storing your password and other pertinent information in the Registry database.

For more information on “How to Enable Automatic Logon in Windows NT” see:
http://www.support.microsoft.com/default.aspx?scid=kb;en-us;97597

III. Utilize your computer’s BIOS settings

Anyone can change your Administrator password if they start your computer up with a Windows Installation CD. We recommend you prevent the possibility of someone unauthorized from booting it from an external hard drive, DVD, or CD, and then changing your administrator password, erasing your disk, or accessing your private documents.

Recommendations: To prevent unauthorized booting from external drives, we recommend you change the boot sequence in your BIOS settings to only boot from the main (C:/) hard drive, and then password protect that BIOS setting.

IMPORTANT: Changing the boot sequence is a function of your hardware settings, NOT PCPHONEHOME™. You should consult your computer's manual for specific information on using the CMOS setup program. An incorrect setting in this critical area of the computer can make the computer non-operative.

While there are other methods to prevent booting from a floppy disk or CD-DVD (physical disk locks to security programs), the most effective solution is enabling the computer's CMOS security features already in your computer. The CMOS is a storage area on your computer where information is retained even when the power is turned off. This important computer information is accessed by a special CMOS setup program.

Pressing a special key sequence (usuualy the DEL key) before Windows starts accesses the CMOS setup program. Once in the CMOS setup, dis-allow booting from the "A" floppy disk drive or CD-ROM/DVD by setting your computer's boot sequence. You have two options: (i) disable the A: drive or CD-ROM/DVD boot ability; or (ii) set the computer's boot sequence from "A:-C:" or "CD-ROM:-C: to "C:-A:" (in other words, boot from the hard disk first).

Finally, enable your computer's setup password to prevent someone from accessing the computer's CMOS settings and changing the boot sequence.

Most computers provide some type of password protection to prevent unauthorized access to the CMOS setup parameters. To enter a CMOS password, start the CMOS program (see above on how to do that), look for a "Security" or "Password" menu item and enter a password for the computer setup. Don't forget to use good security practices by using passwords that are unique to the computer (i.e., don't use passwords used on other computers), and use a combination of upper and lower-case characters, numbers, and words that are difficult to guess by watching the keyboard.

IV. Use Encryption Software to protect your important data.

We recommend that you use some sort of file encryption to protect your valuable data. Try to put all your valuable data into one section or directory and encrypt it. This is much easier (and faster) to encrypting your entire hard drive.

In addition to other commercially available software, Windows XP and 2000 also have file encryption capabilities.

About the Encrypting File System
Microsoft Windows includes the ability to encrypt data directly on volumes that use the NTFS file system so that no other user can use the data. You can encrypt files and folders if you set an attribute in the object's Properties dialog box. This feature is available for Windows XP Professional and Windows 2000 Professional Edition only.
See: http://support.microsoft.com/?kbid=223316

You can use Encrypting File System (EFS) to:
- Encrypt their files
- Access their encrypted files
- Move or rename their encrypted files
- Copy their encrypted files
- Decrypt their files

Check out this link:

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_SEconceptsImpEncrypt.htm