

Chapter

Pointsec PC Overview

1

Pointsec PC is an interactive and remotely managed means of limiting access to sensitive information stored on hard drives. Pointsec PC does this through the use of encryption technology. Encryption is the act of hiding information using a coding formula. This chapter describes encryption with Pointsec PC, and provides a framework for implementing Pointsec PC in an enterprise environment. In addition, you will learn Pointsec PC authentication and security enhancements, the role of Administrators and users, along with Pointsec PC system requirements and services that are useful in conducting daily security administration activities.

Objectives:

- Given Privileged Permissions and Permissions Settings as defined in Pointsec PC, define the role of users and administrators in your organization.
- Considering Pointsec PC's encryption technology, choose the most suitable method for authenticating each user type.
- Install and confirm the installation of Pointsec PC for the Administrator with the installation CDs.

Key Terms

- Local event database
- Local log file

Pointsec Data-Security Technology

A variety of methods and technologies have been employed to secure computers and their contents, including physical controls (cables, locks on power supplies, anchored docking stations, etc.) and electronic means, such as data encryption, user authentication, audit logs, and tracking utilities.

Physical access control is becoming less relevant, with users insisting on portability. There are two general types of computer security: file and disk encryption, and boot protection/authentication.



As defined by Wikipedia.com, to encrypt means to conceal information by means of a code or cipher.

The following graphic illustrates the difference between unprotected data, standard file encryption, and Pointsec PC protection:

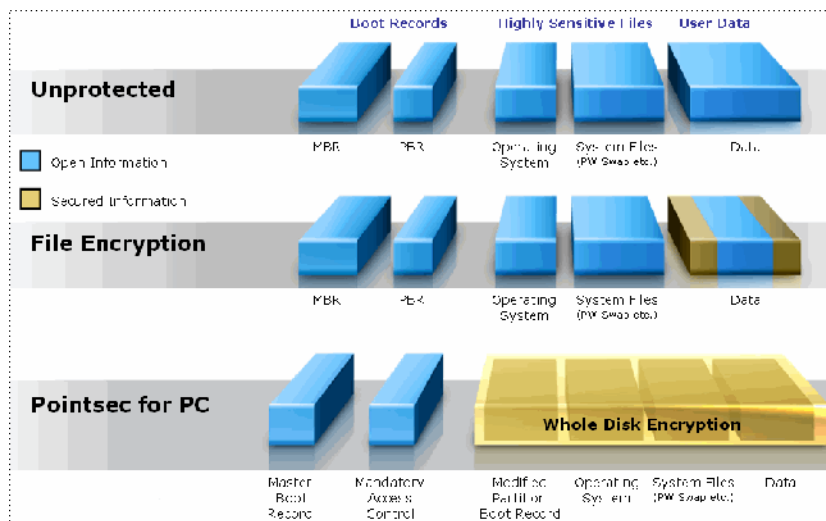


Figure 1-1: Pointsec PC — Complete Data Protection

File and Disk Encryption

File encryption enables users to protect vital data. It is usually easy to implement but is subject to user discretion regarding what to secure, and the willingness of users to consistently follow security procedures. Given this dependence on user compliance, organizations seeking to enforce a security policy often find file encryption insufficient. Unlike file encryption, which leaves security holes, Pointsec PC encrypts the entire disk sector by sector, including system files, temporary files, and even deleted files. The encryption is user-transparent and automatic, so there is no need for user intervention or user training. Because the encryption occurs in the background without noticeable performance loss, there is no user downtime, providing enforceable security that cannot be bypassed by the user.

Boot Protection/Authentication

Boot protection means authenticating users before a computer boots. It prevents the operating system from being undermined by unauthorized persons using any of the widely available password-cracking tools. These tools are plentiful on the Internet, and can be used with devastating effect. Unfortunately, most BIOS-level protection schemes are weak and cannot be tightly linked with disk encryption. Boot protection has the further advantage of providing an effective defense against unauthorized network access via network-connected machines, especially if these machines are linked as part of a VPN.

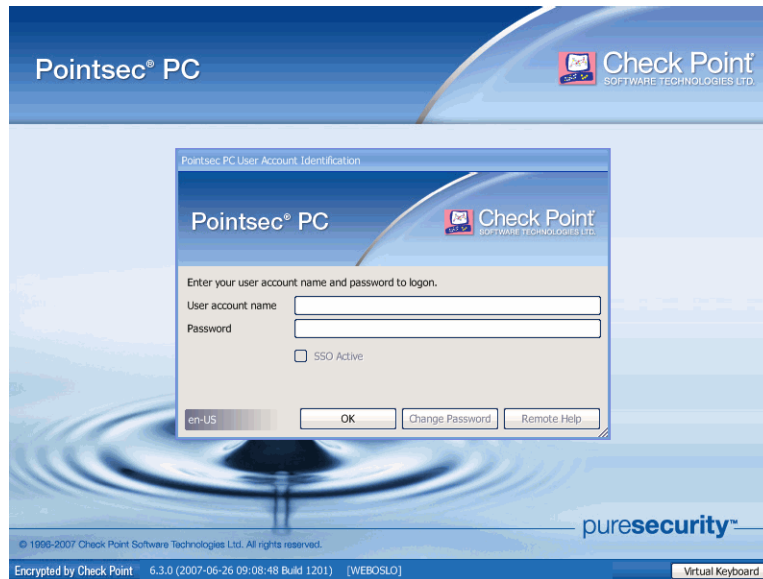


Figure 1-2: Boot Authentication Window

While controlling access to the computer is important, this does not by itself protect the data stored on the disk. For example, a simple boot floppy disk could be used to bypass boot protection. Alternatively, removing the drive and placing it in another computer will make the file accessible to attempted brute-force attacks. Even in those rare cases where the drive itself is secured with a password, the data is not encrypted and is therefore vulnerable to many types of attacks. To secure this data, it must be encrypted. Once encrypted, the credentials used for authenticating are used to encrypt the partition keys; thus making it practically impossible to break the encryption by an unauthorized person.

The Check Point PURE Security Model

With its best-of-breed positioning and extensive product suite, the Check Point PURE Security model offers the most complete protection of an organization's vital data assets.

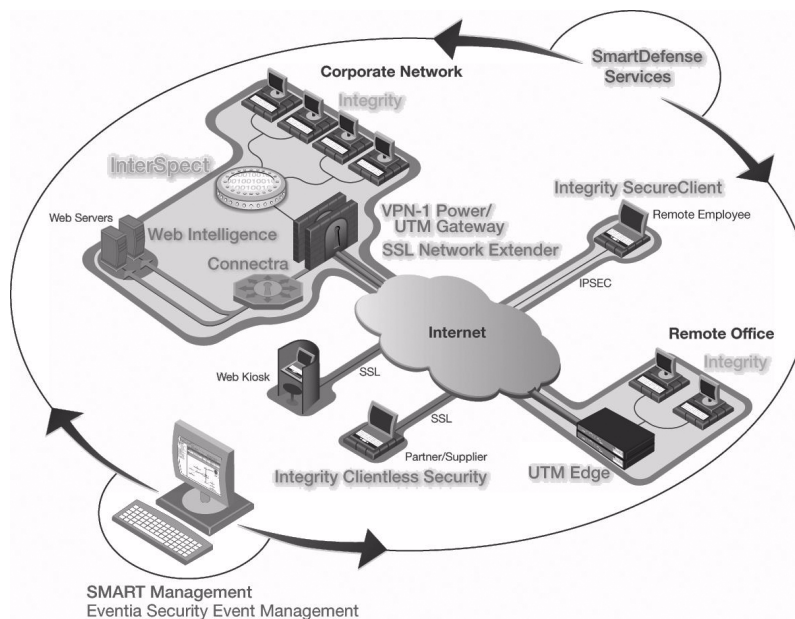


Figure 1-3: The Check Point PURE Security Model

Although the Check Point PURE Security model protects your information assets while users are connected to the network within the boundaries of your environment, there are circumstances where this protection will not extend to your data.

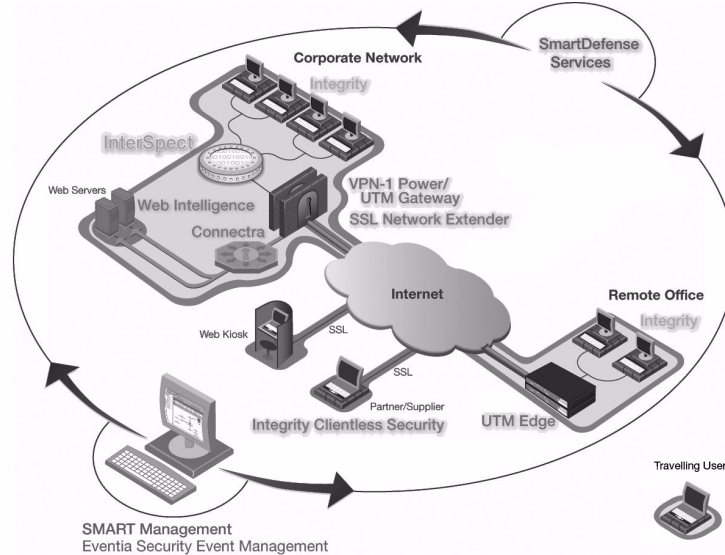


Figure 1-4: Laptop Outside Secure Network

The advent of mobile computing such as laptops, PDA's and data-capable mobile phones has expanded an organization's capabilities by bringing the ability to transfer sensitive data to these devices, but has also provided the potential for catastrophic losses.

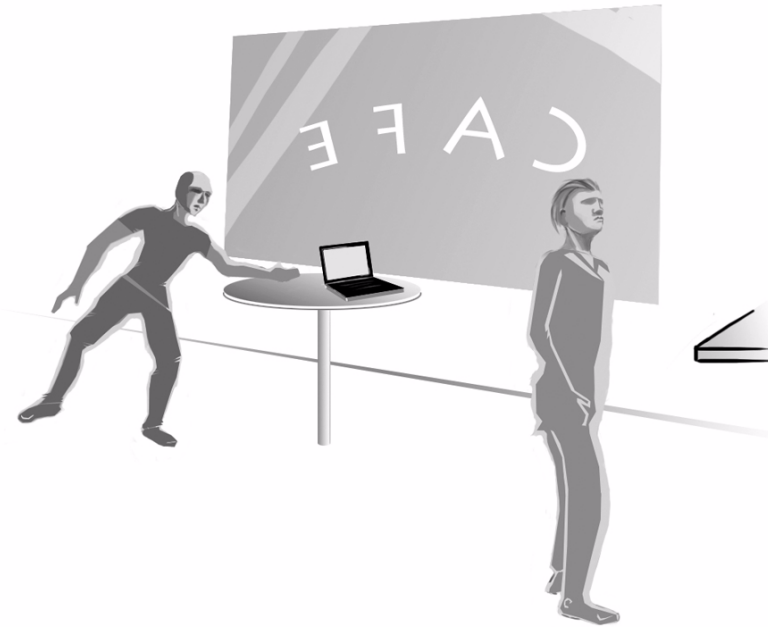


Figure 1-5: Insecure Laptop at an Internet Cafe

Pointsec PC is the hard drive encryption technology from Check Point Software Technologies that protects your sensitive corporate data in such worst-case scenarios.

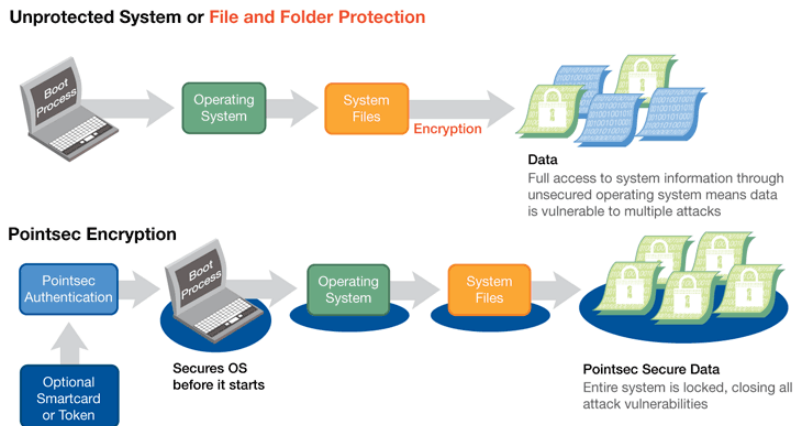


Figure 1-6: Pointsec PC - How It Works

Pointsec PC operates at the boot level, but does not modify the Master Boot Record. Pointsec PC replaces the original boot records upon installation to show the Pointsec PC Preboot Authentication program only. A single MSI installation is available for all Windows versions, using a special profile type.

The encryption of the hard drive is sector-by-sector, allowing for the encryption/decryption process to be done transparently while the operating system is running. The keys used in the encryption/decryption process are dynamically created at boot time.

Pointsec PC distinguishes itself from other hard-drive encryption technologies in that apart from fully encrypting the hard drive, it also uses a two-phase authentication system. In this case, “two-phase” refers to a two-step process which includes how the user authenticates to the Pointsec Preboot Environment (PPBE), and subsequently to the Operating System and Network. This two-step process never uses the same set of decryption information for succeeding logins, since this data is generated dynamically each time the user logs on. The first step takes the login credentials to decrypt a first set of keys necessary for

authenticating to the decryption engine. Then, once authentication to the decryption engine occurs, these keys are used to decrypt a second set of keys for decrypting the data on the hard drive. Once logging in is successful, the key sets are recreated and stored offline.

Consider the following analogy:

Pointsec PC Authentication Example

You need to access some information at the Bozonet Research Institute. Since BRI has strict security policies, these policies will illustrate the “two phase” process. As you drive up to the main gate of the Institute, the guard verifies your car license-plate number, and allows you onto the BRI campus. The license plate information is then used to randomly create an access code that will be your "special access token" into the building. In this case, this information is stored in a fortune cookie. You park your car and take the cookie from the guard, who advises you not to open the cookie until you are at the main gate, warning you that, “Failure to comply with this will mean immediate ejection from the BRI campus.” At the main entrance to the building, another guard takes the cookie from you, verifies that you have not tampered with the cookie, and subsequently breaks it open and enters the fortune into a keypad next to the door, which allows you access to the Institute.

In this analogy, the cookie is your authentication credentials provided at the Pointsec Preboot Authentication screen at boot-up. When entering the “main entrance of the building”, the guard taking the cookie from you is analogous to the second set of keys being generated for access to the data on the hard drive.

Pointsec PC Security Features

Pointsec PC is an enterprise security solution which protects data at-rest against intrusion by employing the use of strong authentication and encryption. It secures desktop and laptop computers from unauthorized physical access, using both boot protection and disk encryption.

Pointsec PC provides the following security functions:

- Operates at the boot level, below the OS level
- No Master Boot Record modification
- Dynamic-key creation upon boot
- Sector-by-sector encryption
- Encryption/decryption processes
- One installation profile caters to all Windows versions
- Single MSI installation
- Strong user authentication
- Secure Remote Help for users who have forgotten their passwords
- Central configuration and administration
- Keyboard lock and screen saver for Windows-based computers
- Limited number of failed login attempts with automatic locking
- Audit logging of events such as successful and failed login attempts

With Pointsec PC, all logical partitions/volumes are boot-protected and encrypted. The careful integration of boot protection and automatic encryption provides a high degree of security with minimal impact on users. Boot protection prevents subversion of the operating system or introduction of rogue programs, while sector-by-sector encryption makes it impossible to copy individual files for brute-force attacks. Disk encryption secures the data even if the disk is removed and installed on a controlled machine. This ensures security by allowing an organization to

determine the security level, instead of leaving it up to the user to see that the information is encrypted.

Disk encryption guarantees unauthorized users cannot access or manipulate information on a protected computer, from either available, erased, or temporary files. Pointsec PC safeguards the operating system and important system files (which often contain clues to passwords for Windows), shared devices, and the network.

Languages Supported in Pointsec PC

Pointsec supports the following languages in the PPBE, in the Pointsec PC Management Console (PCMC), and in the tray application:

- English
- French
- German
- Japanese
- Italian
- Spanish

All other languages into which Pointsec PC has been localized are supported only in the preboot environment and in the tray application.

Managing Pointsec PC

Pointsec PC administration is designed to allow central control of policy and security settings, decentralized deployment and daily administration using the PCMC (see Figure 1-7). Using Pointsec PC profiles, System Administrators are able to install and configure the system, delegate authorization throughout the network, modify the system for local conditions, and assign the properties and authorization of individual users. Simple but powerful local and central logging of system information, group information and individual user account information are permitted.

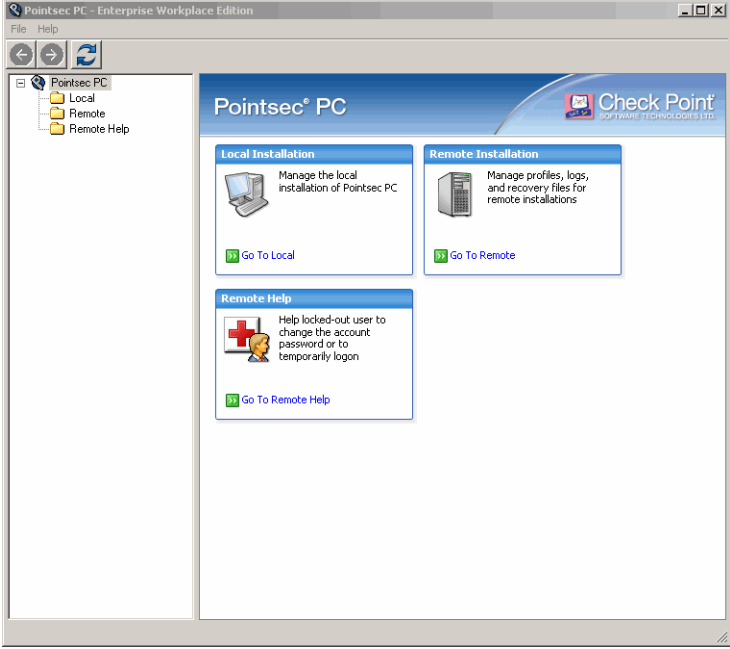


Figure 1-7: Pointsec PC Management Console

Authentication Methods

There is no central authentication database. All authentication occurs against the locally stored database. Pointsec PC supports three user authentication methods: username and password, username and dynamic token, and smartcard with certificate and PIN; and also provides two TCO-enabling process authentications: Windows Integrated Logon (WIL) and Wake-On-LAN (WOL).

The security levels of user authentication scale as follows:

Security Provided	User Authentication Method	Simple Description of Authentication
Good	Username and Password	<p>The username and password provide the identification information and the key material to generate the hash used to authenticate and decrypt the key to the partition keys.</p> <p>These are known only by the user and Pointsec PC.</p>
Better	Username and Dynamic Token	<p>The username and password provide the identification information and the key material to generate the hash used to authenticate and decrypt the key to the partition keys.</p> <p>The Administrator may assign the user a dynamic token.</p>
Better	Pointsec PC Certificate-generator Certificate on smart card with PIN	<p>The smart card detection prompts for PIN input from the user. The PIN is used to authenticate to the smart card, which was associated to the user account. Successful PIN authentication allows the decryption of the 256-bit data blob that is used to decrypt the key to the partition keys.</p> <p>Since this solution does not utilize a PKI for handling certificate revocation and expiration, it does not provide the extended capabilities of a PKI to ensure that expired or revoked user certificates are restricted from authentication.</p>

Table 1-8: Security Levels of Pointsec PC User Authentication Methods

Security Provided	User Authentication Method	Simple Description of Authentication
Best	PKI issued Certificate on smart card with PIN	<p>The smart card detection prompts for PIN input from the user. The PIN is used to authenticate to the smart card, which was associated to the user account. Successful PIN authentication allows the decryption of the 256-bit data blob that is used to decrypt the key to the partition keys.</p> <p>The Pointsec PC Administrator may supply the smart-card/USB token, the information needed to use the card or token, and a temporary username and password to use the first time the Pointsec PC-protected computer is accessed.</p> <p>This method also adds additional controls with certificate linkage to issuing PKI, such that certificate revocation and expiration can ensure user lock out in case of expiration or revocation.</p>

Table 1-8: Security Levels of Pointsec PC User Authentication Methods

The **Best** security for Pointsec PC is achieved when the **Best** user authentication methodology is utilized; however, even **Good** user authentication provides a clear security threshold over any process authentication technology. (See Table 1-8.)

Process Authentication

Windows Integrated Logon (WIL) and Wake On LAN (WOL) are process authentication technologies implemented to avoid user authentication (WIL) and to employ the system-patching process on a temporary basis (WOL). WIL provides an alternative to Preboot Authentication for users who are not managed by Pointsec PC. The procedure is transparent and automatically boots to Microsoft Windows for authentication. Users do not have explicit Pointsec PC credentials and do not require third party tokens or devices for authentication.

Since the PPBE process dynamically generates the encryption blob for the key to the partition keys (see “The Check Point PURE Security Model” on page 24), process authentication is not considered user

authentication. Process authentication does not require any external inputs to initiate the process for decrypting the encryption blob protecting the key to the partition keys.

When WIL is activated, Pointsec PC generates a user account of type WIL in the user database with a copy of the encrypted partition key. Each instance of the WIL user-type created during activation is unique, and random data is used to populate standard entries of the user data (i.e. username). Known elements of the user's Pointsec PC system are utilized to encrypt the partition key(s) for that instance of the WIL user. During the Pointsec PC load process, the status of WIL is checked and if active, then the WIL user account is accessed and the partition key decrypted. A new set of random data is created for the WIL user account. The partition key is subsequently encrypted with known elements used in this process. Thus, no WIL user account is the same (device to device, instance to instance) and the encrypted partition key package changes with each boot.

Since Pointsec PC offers WIL to forego the preboot authentication and launch the operating system directly; this addresses organizations' need to avoid management of another user database, (i.e., as required for Pointsec PC Preboot Authentication with password, dynamic tokens, or smart card).

The capability is centrally controlled, only managed by profile or configuration update in the PCMC regardless of user action. In the event that the capability is turned off, normal preboot authentication operations are active.

WIL and WOL do *not* offer the same level of security as any user authentication, since the process authentication itself provides a more direct approach for attack than user authentication, just by nature of the technology. Therefore, additional security measures are recommended, for example:

- Implement an application to determine if the system utilizing WIL is operating outside of its defined parameters (i.e. removed from the known network. See “The Check Point PURE Security Model” on

page 24). Such an application detects this situation and kills the WIL profile, forcing a lock-out of the user and a reboot to the PPBE.

- Execute Security Policies denying the use of a Windows automatic logon capability.
- Employ defenses for brute force attacks on the Windows logon process.

Recovery

Pointsec PC ensures that data on a system is always recoverable. Since authentication is local to a specific installation, a unique key is created for each device, thereby ensuring that there is no master-key vulnerability. These keys are created automatically at installation and are updated automatically when changes occur, i.e., removing a user profile from a local installation. (See Chapter, “Pointsec PC Management”.) For administrative access to a specific machine, Pointsec PC requires two authorized administrator logins to unlock the administrative mode of a specific machine.



Always keep control of your recovery files, preferably using off-site storage. Data cannot be recovered without it!

Recovery File-Naming Conventions

The recovery-file format is **ComputerName.Domain.com.rec**, where **ComputerName** is the value of the computer name as listed in the Registry key:

```
HKLM\SYSTEM\ CurrentControlSet\ Control\  
ComputerName\ ComputerName
```



You can also run the `hostname` command from the command line to get the recovery filename, i.e., the hostname used as the naming convention of recovery files.

Pointsec PC Authority Levels

Pointsec PC is managed using different levels of authority. It can be managed from the PCMC on any computer that has Pointsec PC installed.

Many businesses define only two levels of authority, i.e., System Administrator, who has full authority, and users whose authority is limited to logging in and receiving remote help. But you can also configure Pointsec PC to have many levels of administration. These levels allow for centralized control of the creation of the profiles that are used to install, update, and uninstall Pointsec PC on client computers, while simultaneously allowing local control of the deployment of those profiles. In this course, we will discuss implementing a hierarchical authority system, which includes a System Administrator, an Administrator, and a user.

System Administrator

Referring to the sample settings below, System Administrators will, among other things, be able to perform the following tasks in the system:

- Create and manage user profiles
- Configure system settings
- Add and remove Administrators and user accounts
- Configure settings for Administrators and user accounts
- Give Remote Help to users who are locked out or have forgotten their passwords

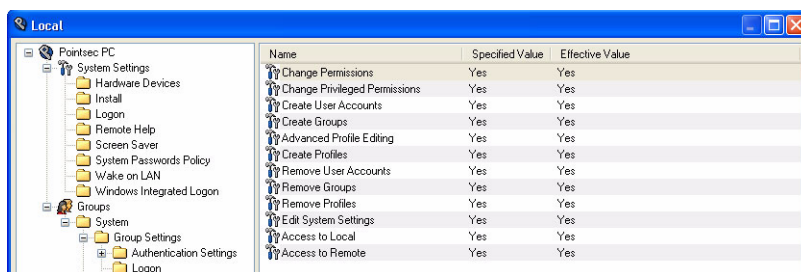


Figure 1-9: System Administrator Example Settings

At least two competent individuals must be designated as System Administrators to manage Pointsec PC and the security of the information it contains. It is imperative that Pointsec PC System Administrators receive adequate training and are not careless, willfully negligent, or hostile. Pointsec PC System Administrative personnel must keep their authentication data private.

Administrator

Administrators should be given more limited authority in relation to what has been defined for the System Administrator in the system settings. An Administrator can add, remove, and change certain settings for specific users. They are not allowed to work with users who have higher administration privileges than they do, nor can they raise their own authorization level. Administrators are usually allowed to provide Remote Help and to modify profiles.

By default, Pointsec PC Administrators have the same authority as users. The System Administrator determines the amount of authority an Administrator has by configuring the authority settings in the System Settings dialog box.

User

Users have limited authority, according to what has been defined by the System Administrator in the system settings. Each user is assigned an

account with a unique user identity and password that together authorize access to the entire hard disk.

Typical Role Permissions

The following table lists **Privileged Permissions**, **Permissions** and **Remote Help** settings for a possible structure with Pointsec PC user accounts, Administrators, and System Administrators. This structure provides a good level of security, but you will probably want to define your own structure. For more information about these settings, see chapter “The Pointsec PC Management Console” in this coursebook.

Privileged Permissions	User	Administrator	System Administrator
Change Permissions for User Accounts			X
Change Privileged Permissions			X
Create and Edit User Accounts			X
Create and Edit Groups			X
Create Profiles			X
Remove User Accounts			X
Remove Groups			X
Remove Profiles			X
Edit System Settings			X

Permissions	User	Administrator	System Administrator
Change Password			X

Permissions	User	Administrator	System Administrator
Change Single Sign-On			X
View Logs		X	X
Uninstall		X	X
Provide Remote Help		X	X
Management Console Logon		X	X
Edit System Settings			X
Create Recovery Media			X

Permissions/ Remote Help	User	Administrator	System Administrator
Provide 'Reset Password'		X	X
Provide 'One Time Logon'		X	X
Receive 'Reset Password'	X		
Receive 'One Time Logon'	X		

Automatic Logging and Centralized Auditing

Pointsec PC can create and store event logs in a central log file that can be made available to a central management point of access. Pointsec PC also maintains local log files on each Pointsec PC-protected local machine.

Pointsec PC events are logged in one or more of the following:

- Local event database
- Local log file
- Central log file
- Windows Event Log

For more information, see chapter “Pointsec PC Log Management”.

Remote Help

Pointsec PC includes a Remote Help function that gives Administrators the ability to help users with lost password information without the user being online. This is done using a secure Dynamic Challenge/Response procedure.



Remember to validate the end user before using Remote Help!

Pointsec PC Licensing

Pointsec PC is sold per seat. Licensing is provided based on the number of seats that are sold. For all licensing requests, contact Check Point Account Services:

<http://www.checkpoint.com/services/contact/index.html>

For more information about licensing for Pointsec PC, see the following:

<http://www.checkpoint.com/services/education/atc/tools.html>

Pointsec PC Components

The basic installation of Pointsec PC on an endpoint is comprised of the following components, and described below:

- Pointsec PC Database
- Pointsec PC Boot Authentication

Pointsec PC Database

The local Pointsec PC database is a closed database allocated from 2 MB of contiguous space, and is encrypted using a 512-bit key. The database is created from the Pointsec PC installation profile, and stores all of the users and groups that have access to the local computer. Users authenticate to the local database at boot authentication. The database can be viewed by clicking **PCMC > View Local Event Database**:

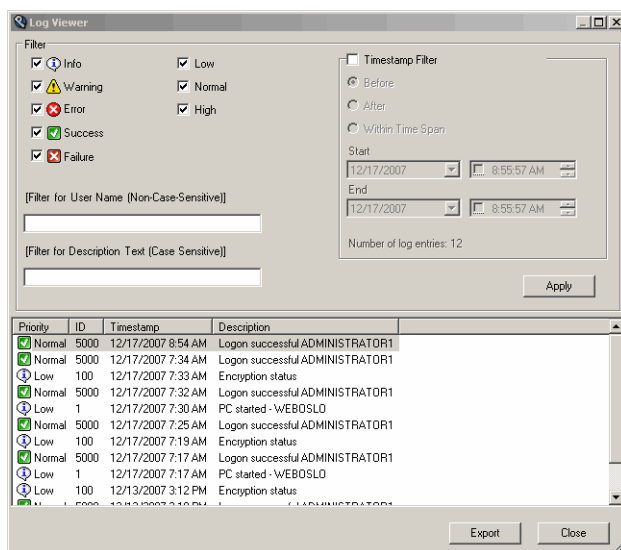


Figure 1-10: Log Viewer

Pointsec PC Boot Authentication

Being authenticated means being verified by Pointsec PC as someone who is authorized to use a specific computer. When you switch on or restart a Pointsec PC-protected computer, the **User Identification** dialog box opens.

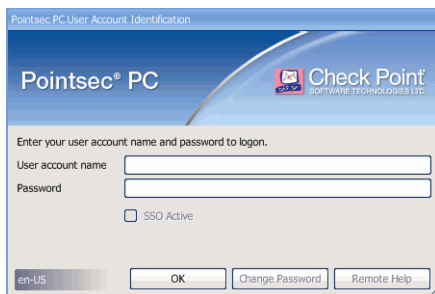


Figure 1-11: Preboot Authentication

The preboot-authentication program, also known as the **Pointsec Multi Factor Authentication Engine (MFAE)**, replaces the standard hard-drive boot records. This allows for the preboot-authentication login window to appear before boot.

Here you must enter a valid username and password. Pointsec PC verifies that you are authorized to access the computer and allows the computer to start.

The MFAE loads after BIOS and the low-level boot record via a modified-partition boot record, so Pointsec PC authentication is performed before the operating system starts.

The Pointsec PC Preboot Environment (PPBE) is comprised of the following components:

- 32-bit secure operating system
- VESA graphics, .jpg background
- Keyboard drivers

- Mouse drivers
- Support for virtual keyboard in PPBE
- Pointsec PC supports using the tablet PC pen in preboot on the following systems:
 - IBM X41
 - HP TC 1100
 - HP TC 4200
 - Toshiba Portégé M200.
- MFAE
- Pointsec PC smart-card drivers
- Pointsec PC Reader Drivers

It is possible to synchronize the Pointsec PC preboot and Windows passwords. The Windows password can be set to be the Pointsec PC preboot password, or vice versa. And anytime the password is reset, the preboot and Windows passwords will be reset respectively. See chapter “Pointsec Management Console” for more information.

In addition, Pointsec PC can now be configured to require preboot authentication if hardware changes are detected on a system running Windows Integrated Logon, or is based on available IP addresses.

Pointsec PC Management Console

The Pointsec PC Management Console (PCMC) is available in an administrative or master installation, or when an Administrator logs into a user's machine. The PCMC is divided into three primary sections: Local, Remote and Remote Help. Each section is described in the following list:

- **Local** — This section is used to change local settings, manage local logs, check local status, etc.
- **Remote** — Here, the Pointsec PC Administrator can create and deploy configuration files (profiles) that will affect remote computers.
- **Remote Help** — This section is used to perform Remote Help and one-time login tasks.

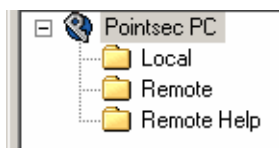


Figure 1-12: Pointsec PC Management Menu

The PCMC works with the Pointsec PC program via the **PCMCUtil.dll** driver and the **Prot_ins.sys** database:

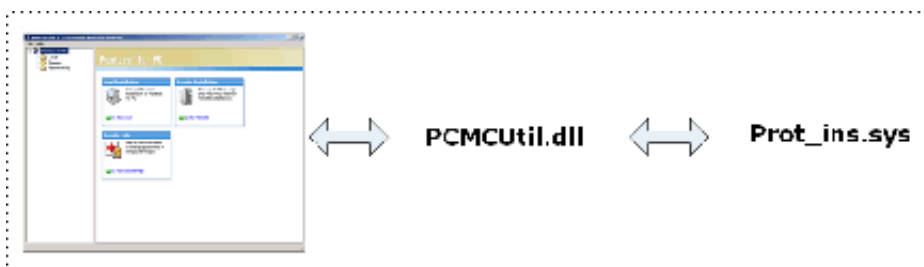


Figure 1-13: Driver/Database Interaction

- **PCMC** (system settings) — Creates, updates and manages profiles, locally and remotely; client needs **.Net Framework** installed.
- **PCMUtil.dll** (driver) — The driver encrypts/decrypts profiles, works with the database in authentication, and imports local profiles into the database.
- **Prot_ins.sys** database (SA) — This utility stores the profile information used in authentication and the token drivers. The database has been extended from its size in earlier versions of 1.7 MB to 2.0 MB.

Pointsec PC Encryption-Key Generation

Since the authenticating credentials are used for encryption, Pointsec PC encryption keys are created after the first reboot. Individual keys are created for each partition, to provide the highest level of security. An AES 256-bit algorithm is used to generate the keys for encryption.

Initial Encryption of the Hard Drive

Encryption takes place *only* after Pointsec PC off-loads the Recovery file from the local machine. Regardless of how much information is on the hard drive, the encryption rate is approximately 10 GB per hour. This functions as a throttled background service, allowing the workstation user to continue to work while the drive is encrypting. Mousing over the system-tray icon shows encryption status:

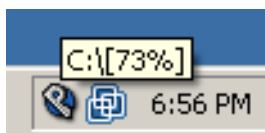


Figure 1-14: Encryption Status

Common Criteria EAL4 Configuration Requirements

The validation of Pointsec PC is done in a specific secure configuration. To use Pointsec PC as a validated product, this configuration must be used on the installed computer. To properly implement a Common Criteria (CC) EAL4 validated configuration of Pointsec PC, specific settings must be configured in the profile that will be deployed.



According to Wikipedia, “The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999...The intent of the higher levels is to provide higher confidence that the system's principle security features are reliably implemented.”

The algorithms and key sizes allowed in a CC configuration are:

- 3DES 168-bit.
- AES 256-bit.

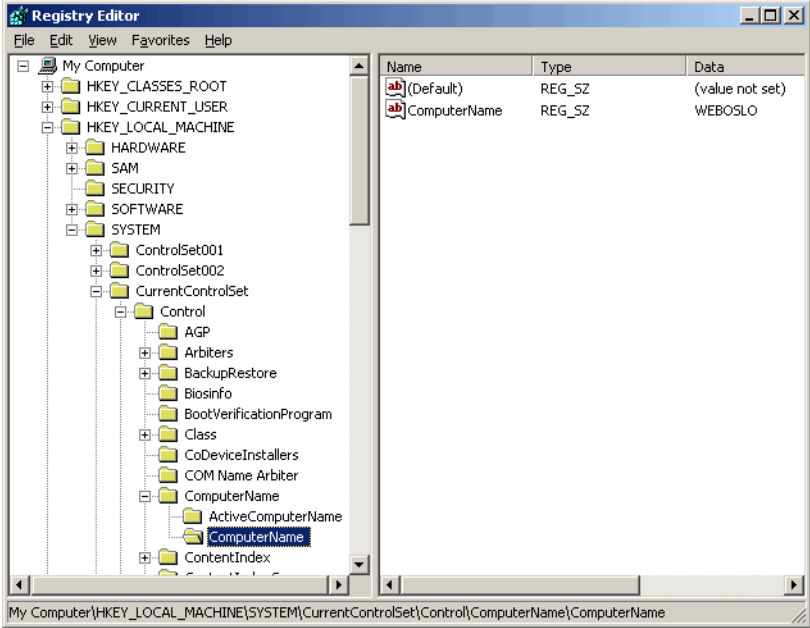


Figure 1-15: Registry Key-Naming Information

Services and Processes

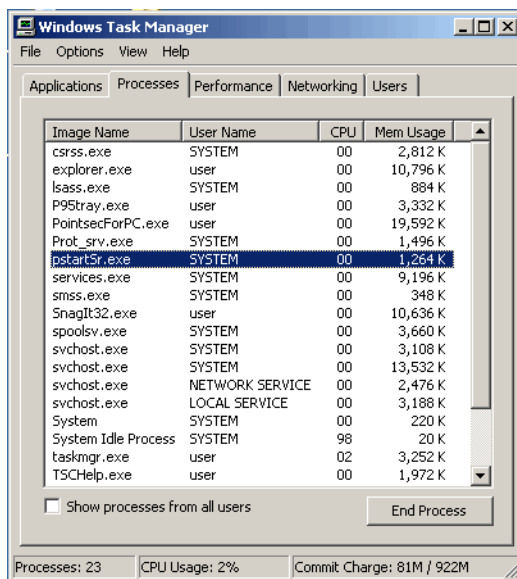


Figure 1-16: Pointsec PC Processes in Task Manager

Pointsec PC runs three services on the local machine:

- **PROT_SRV.EXE** — provides encryption and decryption during installation and uninstallation
- **PstartSr.EXE** — allows Pointsec PC to push recovery files and poll for update profiles
- **P95tray.EXE** — the taskbar application

Pointsec PC Monitoring — P95Tray.exe

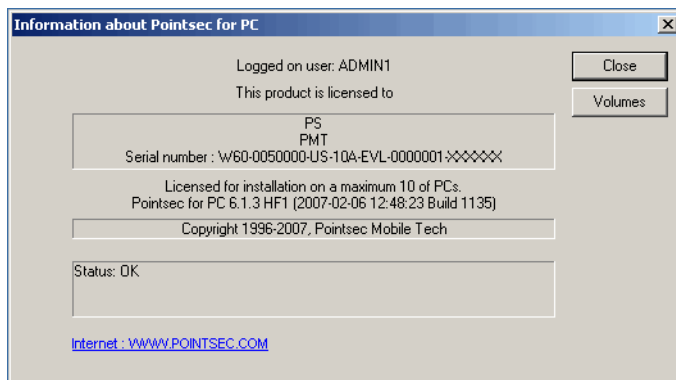


Figure 1-17: P95Tray.exe Interface



Figure 1-18: P95Tray.exe Icon

P95Tray.exe is the monitoring program that is accessible for end users. Any user on the machine can use this to:

- Check encryption status (when Pointsec PC is first installing and encrypting).
- Activate the screen saver to lock the workstation.
- Select the language in the PPBE or Windows (more than 25 languages supported).

Additionally, Administrators can access this to change credentials on the local system.

System Requirements

The following sections describe operating system, memory, and disk-space requirements and limitations.

Supported Operating Systems

Pointsec PC is supported when installed on an x86-compatible computer with:

- Microsoft Windows Vista (32-bit).
- Microsoft Windows XP Tablet PC Edition.
- Microsoft Windows Server 2003 (all variants and SPs) is supported on PC/desktop hardware only.
- Microsoft Windows 2000 Professional SP4 UR1.
- Microsoft Windows XP Professional (SP1 and SP2, SP2 recommended).

Unsupported Operating Systems

Pointsec PC is *not* supported when installed on a computer with:

- Microsoft Windows XP Home (all variants and SPs).
- Microsoft Windows Media Center Edition (all variants and SPs).



Microsoft .NET Framework 2.0 or later is required to be able to use the PCMC.

Operating-System Requirements/Limitations

Stripe/Volume Sets

On Windows 2000/Windows XP, Pointsec PC should not be installed on partitions that are part of stripe or volume sets.

Compressed Root Directory

Pointsec PC cannot be installed if the root directory is compressed. The root directory must be decompressed before Pointsec PC is installed. However, subdirectories of the root directory may be compressed.

Windows 2000 User Account Registry Permission Requirements

To install, upgrade, change language, import, and remove profiles on a Windows 2000 computer, a user account needs the following Registry permissions:

- Query value
- Set value
- Create
- subkey
- Enumerate subkey
- Notify
- Create link
- Read control
- Delete

Memory and Disk-Space Requirements

The current memory and disk-space requirements are as follows:

Operating System	Memory	Condition
Windows Vista	512 MB RAM	100 MB disk space, where 2 MB must be contiguous free space
Windows XP	128 MB RAM	100 MB disk space, where 2 MB must be contiguous free space

Table 1-19: Pointsec PC Operating System and Memory Requirements

Operating System	Memory	Condition
Windows 2000	64 MB RAM	100 MB disk space, where 2 MB must be contiguous free space
Windows Server 2003 (Not server hardware)	64 MB RAM	100 MB disk space, where 2 MB must be contiguous free space
Windows XP Tablet Edition	128 MB RAM	100 MB disk space, where 2 MB must be contiguous free space

Table 1-19: Pointsec PC Operating System and Memory Requirements



If 2 MB of continuous space is not available, the installation will fail. In general, it is considered good practice to avoid fragmented disks to enhance overall performance. It is also considered good practice to defragment disks prior to installing Pointsec PC.

The disk-encryption process does not require extra space on the hard disk.

File Systems/Volumes/OS Upgrades

The following list describes hard-disk limitations for Pointsec PC:

- **Resizing partitions** — Never use any disk-partition editing software with Pointsec PC installed on the workstation. If you need to resize a partition, remove Pointsec PC first, and then resize the partition.
- **Overlapping partitions** — When moving disks between computers where the computers have different head counts (i.e., $H=64 > H=16$), fdisk may produce overlapping partitions. Pointsec PC will not start encryption if overlapping partitions are found. In addition, this problem can sometimes occur on machines with multiple volumes.

- **Disk volume without drive letter** — If the system partition is not accessible using a drive letter when Pointsec PC is installed, necessary changes cannot be made, and the installation cannot be completed.
- **Disk utilities** — Do not use disk utilities to change file systems or resize any volumes on the hard disk if Pointsec PC is installed. Doing so may lead to an unusable system.
- **OS Upgrades** — Do not upgrade from one operating-system version to another while Pointsec PC is installed, i.e., upgrading from Windows 2000 to Windows XP. This may lead to an unusable system. (However, you can install service-pack upgrades.)



Do not modify the **Pointsec for PC.msi** package in any way, i.e., by using transforms. Modification of the **Pointsec for PC.msi** package invalidates the supportability of the product.

Software Incompatibilities

- **Remote Help malfunctions on slaved hard disk drives** — Remote Help's remote-password change and one-time login do not function on slaved hard drives.
- **Antivirus software** — Pointsec PC is not fully compatible with some antivirus software. The encryption process performed by Pointsec PC is performed in the background and does not affect computer performance noticeably. However, if antivirus software runs a disk scan while Pointsec PC is encrypting the disk, performance will be impaired. During the encryption process, BIOS antivirus-feature functionality should be disabled. If active, it will cause the system to hang when reloading from suspend mode.
- **Pointsec PC and VMware** — Pointsec PC does not support VMware in a production environment. VMware is supported only for testing and demonstrations. In addition, note that the use of smart

cards and smart card readers together with Pointsec PC is severely restricted in VMware sessions.

Known Limitations

Refer to the following list for known Pointsec PC limitations:

- **Deployment software** — When Pointsec PC is installed on a client using deployment software such as SMS or Tivoli, the software must be run as LOCAL_SYSTEM and have **Interact with desktop** activated. If the software is run as a normal user account, the installation will fail.
- **SATA CD/DVD devices** — These devices are not supported in the Alternative Boot Menu.
- **Dual booting** — Pointsec PC does not support dual-boot environments.
- **Multiple hard disks** — Up to six hard disks are supported, which together can have a maximum total of 12 volumes protected by Pointsec PC.
- **Recovery and hibernation** — Do not attempt to perform recovery on a hibernated machine.
- **Hidden volumes** — Pointsec PC cannot be installed on hidden volumes.
- **Mounted volumes/dynamic disks** — Mounted volumes/dynamic disks are not supported.
- **USB and CD-ROM limitations** — Devices with boot media should be removed while the Pointsec PC Preboot Environment is loading. USB devices, bootable CD-ROMs, and bootable DVD-

ROMS are not supported in the system during the preboot authentication.



For the complete list of limitations, see the Pointsec PC 6.3 Release Notes.

