Note - Before beginning the installation, read the latest available version of these release notes at: http://www.checkpoint.com/support/

In This Document

Information About This Release page 2
What's New page 5
Upgrading Components page 8
Known Limitations page 9
Resolved Limitations page 28
Documentation Feedback page 47
Information About This Release

Endpoint Security combines firewall, network access control, program control, anti-malware, data security, and remote access, enabling administrators to deploy endpoint security with a single deployment utility. This document contains important information not included in the documentation. Review this information before setting up Endpoint Security.

Note - The Endpoint Security Distribution Utility does not, at this time, verify or perform any validation on installation packages. Please ensure that any installation packages used to install Endpoint Security features are obtained from a trusted source.

Build Numbers

The following table lists all Endpoint Security Distribution Utility products, and their current build numbers as distributed on the product CD. To verify each product's build number, use the appropriate command format or direction within the GUI.

<table>
<thead>
<tr>
<th>Product</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Client Deployment Utility</td>
<td>493000154</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>1349</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>493000133</td>
</tr>
<tr>
<td>Secure Access</td>
<td>72077000_1</td>
</tr>
</tbody>
</table>
General System Requirements

In This Section

Minimum Hardware Requirements
Software Environment
Operating System
Full Disk Encryption - Specific Requirements

Minimum Hardware Requirements

- **CPU**: Pentium III 450 MHz
- **RAM**: 500 MB
- **Free Disk Space**: 300 MB

Software Environment

- Microsoft .NET Framework 2.0

Operating System

<table>
<thead>
<tr>
<th>Full Disk Encryption:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP Professional SP1, SP2, SP3 (SP2 recommended)</td>
</tr>
<tr>
<td>Microsoft Windows Vista (32-bit only): Ultimate, Business, or Enterprise</td>
</tr>
<tr>
<td>Microsoft Windows Vista (32-bit only) SP1: Ultimate, Business, or Enterprise</td>
</tr>
<tr>
<td>Microsoft Windows XP Tablet PC Edition</td>
</tr>
<tr>
<td>Microsoft Windows Server 2003, for all variants and SPs, on client computers only (not servers)</td>
</tr>
<tr>
<td>Microsoft Windows 2000 Professional SP4 UR1</td>
</tr>
</tbody>
</table>

Exceptions:

Full Disk Encryption is NOT supported when installed on:

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

In addition, you cannot use Full Disk Encryption to encrypt partitions that are part of RAID stripe or volume sets.

<table>
<thead>
<tr>
<th>Media Encryption:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP SP2, SP3</td>
</tr>
<tr>
<td>Windows 2000 SP4</td>
</tr>
<tr>
<td>Windows Vista Enterprise</td>
</tr>
<tr>
<td>Windows Vista Enterprise SP1</td>
</tr>
<tr>
<td>Windows 2003 Server SP2</td>
</tr>
<tr>
<td>Windows 2000 Server SP4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Access:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP SP2, SP3</td>
</tr>
</tbody>
</table>
### Full Disk Encryption - Specific Requirements

<table>
<thead>
<tr>
<th>Stripe/Volume Sets</th>
<th>Full Disk Encryption should not be installed on partitions that are part of stripe or volume sets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compressed Root Directory</td>
<td>Full Disk Encryption cannot be installed if the root-directory (or root directories) is/are compressed. The root directory must be decompressed before Full Disk Encryption is installed. However, subdirectories of the root directory may be compressed.</td>
</tr>
<tr>
<td>Windows User Account Installation and Uninstallation</td>
<td>In order to install or uninstall Full Disk Encryption, the user account executing the action (either directly, through “Run As…”, or as a service) must be authorized to perform installations, this usually means having Administrator permissions.</td>
</tr>
<tr>
<td>Windows User Account Registry Permission Requirements</td>
<td>In order to install, upgrade, change language and import profiles on a Windows 2000 PC, a user account needs the following registry permissions: Query value, Set value, Create subkey, Enumerate subkey, Notify, Create link, and Read control. In order to remove on a Windows 2000 PC, a user account needs the above registry permissions plus Delete.</td>
</tr>
<tr>
<td>Resizing Partitions</td>
<td>Never use any disk partition editing software when Full Disk Encryption is installed on the workstation. If you need to resize a partition, remove Full Disk Encryption completely first and then resize the partition.</td>
</tr>
<tr>
<td>Overlapping Partitions</td>
<td>When moving disks between computers where the computers have different head counts (e.g. H=64 --&gt; H=16) FDISK may produce overlapping partitions. The operating system does not notice this. Full Disk Encryption will not start encryption if overlapping partitions are found. This problem can sometimes occur on machines with multiple volumes.</td>
</tr>
<tr>
<td>System on Volume without Drive Letter</td>
<td>If the system partition is not accessible using a drive letter when Full Disk Encryption is installed, necessary changes cannot be made; and the installation cannot be completed.</td>
</tr>
<tr>
<td>Disk Utilities</td>
<td>Do not use disk utilities to change file systems or resize any volumes on the hard disk if Full Disk Encryption is installed, doing so may lead to an unusable system.</td>
</tr>
<tr>
<td>OS Upgrades</td>
<td>Do not upgrade from one operating system version to another while Full Disk Encryption is installed, for example upgrading from Windows 2000 to Windows XP. This may lead to an unusable system. However, you can install hotfix upgrades.</td>
</tr>
</tbody>
</table>
What’s New

The following sections offer a brief overview of the features and functionality offered by Endpoint Security Distribution Utility NGX R65.

In This Section:

Unified Endpoint Security Solution  page 5
One Console For Simplified Management  page 5
Endpoint Security Deployment Utility  page 5
Data Security  page 6
Secure Access  page 7
Endpoint Security License Server  page 7
SmartCenter for Pointsec - WebRH  page 7

Unified Endpoint Security Solution

Check Point Endpoint Security™ is the first and only single agent that combines all essential components for total security on the endpoint: highest-rated firewall, antivirus, anti-spyware, full disk encryption, media encryption with port protection, network access control (NAC), program control and VPN.

It protects PCs and eliminates the need to deploy and manage multiple agents, reducing total cost of ownership. Check Point Endpoint Security is the only solution that includes both data security to prevent data loss and theft and a VPN client for secure remote communications.

One Console For Simplified Management

Endpoint Security features a powerful, unified management system that reduces overall cost and complexity by enabling administrators to deploy, manage, and monitor security policy for thousands of endpoints across a distributed organization—all from a single console. The management server installs in minutes, and the agent software can be deployed quickly without end-user involvement. It also provides powerful tools to enhance and customize endpoint security policies specific to the needs of an organization and enables distinct policies to be applied automatically to endpoints as they change networks, locations, and access points.

- Monitor, analyze, and report on security events from a single administrative console
- Easy to deploy and manage with one simple installation
- Unified with Check Point SMART management to enable monitoring, analysis, and reporting of endpoint security events from SmartCenter™, Provider-1®, and Eventia® management systems

Endpoint Security Deployment Utility

Check Point Endpoint Security™ includes a deployment utility that allows administrators to deploy customized installations to endpoint machines quickly and easily with a single installation process. Administrators typically use "silent" installation packages to automatically install pre-configured Endpoint Security Client deployments without the need for user intervention.

Administrators can create silent installation packages using the Endpoint Security Distribution Utility. Administrators can also use the Endpoint Security Distribution Utility to install licensed, working deployments or evaluation deployments on local computers.
Data Security

Endpoint Security includes market-leading data security features to provide data protection through an efficient blend of full-disk encryption, access control, port management, and removable media encryption.

Full Disk Encryption (FDE)

Based on market-leading technologies, Endpoint Security Full Disk Encryption™ (FDE) is proven in enterprises, businesses and government agencies around the world, providing the highest level of data security for laptops and PCs through a combination of pre-boot authentication and strong encryption algorithms. Full Disk Encryption is now fully integrated in the Endpoint Security Client and can be easily installed using the new Deployment Utility. The enhanced feature/functionality in this release includes:

Simplified Administration:
- Temporary user account management
- Pre-boot environment debug log
- Start menu MSI shortcut switch for FDE
- Install Windows component only
- Profile backward compatibility

Increased Flexibility:
- Dual boot support (Windows and Redhat Linux)
- Serial over LAN

Improved Feature Set:
- Dynamic hard disk encryption
- License server / License enforcement

Media Encryption

Media Encryption prevents unauthorized copying of sensitive data by combining port and device management, content filtering and centralized auditing with robust media encryption. Media Encryption plugs potential leak points and logs data movement to and from any plug and play devices, providing comprehensive control of security policies.

Key Features:
- Centrally managed port control and content filtering
- Removable media encryption such as flash drives, CDs and DVDs, etc.
- Enforced content and virus scan
- Granular control of removable media by type, brand, or model
- Centralized auditing and reporting
Secure Access

The Secure Access features provide iron-clad endpoint client security while minimizing user intervention.

Firewall

Check Point Endpoint Security features an industry-leading firewall that blocks unwanted traffic, prevents malware from infecting endpoint systems, and makes endpoints invisible to hackers.

- Uses “stealth mode” to make endpoints invisible to hackers scanning for vulnerable systems
- Controls which applications are allowed network access
- Ensures that approved programs cannot be spoofed, tampered with, or hijacked

Malware Protection

Check Point Endpoint Security terminates viruses, spyware, keystroke loggers, Trojans, and other malicious programs before they can damage endpoint systems. Backed by the industry’s fastest security update services.

- Comprehensive antivirus, anti-spyware, and host intrusion prevention
- Hourly updates provide immediate protection against the latest spyware, worms, Trojans and other malware

VPN

Only Check Point Endpoint Security unifies advanced remote access as an indispensable part of endpoint security.

- IPSec VPN client based on the award-winning VPN-1® and SecureClient™ technologies
- Includes flexible connectivity options and supports multiple authentication schemes
- Applies full security policies to remote access traffic

Endpoint Security License Server

The Endpoint Security License Server provides license enforcement and tracking capabilities for Endpoint Security clients. Endpoint Security License Server monitors and manages installed licenses and activated licenses, including keeping track licensed assigned to specific clients.

SmartCenter for Pointsec - WebRH

SmartCenter for Pointsec - WebRH provides a hierarchical remote help management solution for Full Disk Encryption and Media Encryption.
Upgrading Components

The Endpoint Security Deployment Utility automatically upgrades previously installed versions of the following components:

- Full Disk Encryption
- Media Encryption
- Secure Access

This section presents the allowable upgrade paths for each of these components.

Full Disk Encryption

- Full Disk Encryption 4.1 sr 2.14 or later
- Full Disk Encryption 4.2 sr 1.4 or later
- Full Disk Encryption 4.3
- Full Disk Encryption 5.x.x
- Full Disk Encryption 6.x.x (but not directly from 6.0.0 see “Known Limitations” on page 9).

Media Encryption

- Pointsec Protector version 4.51 and higher
- Files encrypted with Media Encryption version 2.0 SR1 and higher are compatible with the current version

Secure Access

Integrity/Endpoint Security versions 6, 6.5 and 7
Known Limitations

In This Section

- Endpoint Security Deployment Utility page 9
- Full Disk Encryption page 11
- Media Encryption page 25
- Secure Access page 26

Endpoint Security Deployment Utility

00423669 Loss of Internet connectivity may be experienced after installing Microsoft patch KB951748. See sk35506 before installing the patch.

00405921 This version of the Deployment Utility does not perform any security validations for installers and packages. Ensure that these items originate from a trusted source.

00406933 During the installation process, a reboot request may appear due to "changes in logon configuration" (The message title reads "Fingerprint Logon"). You MUST click NO to this request. If you click Yes, the installation will not continue.

00407205 The current version of the Deployment Utility does not verify that the input path is valid. Users should manually verify path validity before proceeding.

00407441 The current version of the Deployment Utility does not verify that there is sufficient disk space to perform the product installation. A full installation requires approximately 300 MB of free disk space. Users should verify that sufficient disk space prior to running the Deployment Utility.

00408503 The Deployment Utility does not verify that there is no other Deployment Utility running on the local machine. This may result in installation failures or problematic updates.

00409111 The option to save to a file appears in error after a silent installation using a predefined installation package. You can safely ignore this option.

00409970 Failure to clearly specify the fully qualified network path to the Full Disk Encryption will result in failure to import the correct files into the installation package. The specified network path must be accessible from the endpoint computer.

00409982 Specifying an incorrect. msi file for a Full Disk Encryption installation may cause the Deployment Utility to become unstable.

00410928 The current version of the Deployment Utility does not verify the currently installed version of any products prior to installation. It will automatically "upgrade" any previously installed version.

00411030 When using the Deployment Utility to install a licensed working version or an evaluation on a local computer, the both installation type configuration fields remain available. Make certain that you configure the correct configuration type.
00411913 Using End Point Security and McAfee VirusScan Enterprise Version 8.5i together on the same computer may result in performance issues due to CPU overload.

00411930 Using Endpoint Security together with Norton 360 on the same endpoint machine is not supported.

00412046 In the event that a Secure Access upgrade installation fails, the Deployment Utility reports it as a successful installation. The existing installed version remains intact.

00412611 In some cases, as a result of server configurations, a Media Encryption upgrade installation may fail. In such cases, the existing installed version will remain intact.

00412822 The Deployment Utility does NOT validate user-entered data. Incorrect data will result in an invalid file and the installation will fail. This is also true for incorrect or invalid license data.

00412858 The silent installation package incorrectly presents an option to save the current settings to an .ini file. You MUST ignore this option. Use of the option may cause the deployment utility to provide an error message. If this occurs, simply ignore the message and reboot the computer. All components will be installed correctly.

00412878 This version of the Deployment Utility does not check for the presence of the Vista operating system, even though Secure Access does not currently support it. Users should not attempt to use the Deployment Utility to install Secure Access on Vista platforms.

If users run the Deployment Utility on a Vista platform, Secure Access installation will fail, but the rest of the features will install correctly and behave normally.

00419415 You should always run the Deployment Utility with administrator permissions when using Windows Vista.

00422844 When installing Endpoint Security Client using a Group Policy, you must perform the reboot using GPO commands. To do so, perform the following steps:
1. Create a local copy for the cpdefault.ini file. (e.g. c:\my_cpdefault.ini).
2. Edit the local copy and set the PkgUserRebootType parameter to 3.
3. Execute the CPEndpointSecurity.exe -f c:\m_cpdefault.ini command to create an installation package.
4. Add the installation package executable to the login script.
5. Distribute the batch file using the GPO login script.
6. Perform a GPO reboot after executing the installation package.

00452628 In this version, Installation files are not digitally signed.
Full Disk Encryption

Software, Hardware, and Operating System Considerations

Total Security Package License: The License Server does not support the Total Security Package license for FDE. To activate an FDE license using the License Server, you must obtain a license file containing only Full Disk Encryption.

Stripe/Volume Sets: On Windows 2000/Windows XP, Full Disk Encryption should not be installed on partitions that are part of stripe or volume sets.

Compressed Root Directory: Full Disk Encryption cannot be installed if the root-directory (or root directories) is/are compressed. The root directory must be decompressed before Full Disk Encryption is installed. However, subdirectories of the root directory may be compressed.

Windows User Account - Installation and Uninstallation: In order to install or uninstall Full Disk Encryption, the user account executing the action (either directly, through “Run As…”, or as a service) must be authorized to perform installations, this usually means having Administrator permissions.

Windows User Account Registry Permission Requirements: In order to install, upgrade, change language and import profiles on a Windows 2000 PC, a user account needs the following registry permissions: Query value, Set value, Create subkey, Enumerate subkey, Notify, Create link, and Read control.

In order to remove on a Windows 2000 PC, a user account needs the above registry permissions plus Delete.

Strong Recommendation - Windows Integrated Logon (WIL): When implementing Windows Integrated Logon (WIL), weigh the total cost of ownership (TCO) impact of implementing Pre-Boot Authentication against the need for strong security when accessing the encrypted data at rest. WIL simplifies the user’s experience when logging on to encrypted machines at the cost of limiting the strength of the PC’s security configuration.

Consider using Single Sign-On (SSO) in conjunction with proper Pre-Boot Authentication as an alternative to WIL. Carefully weigh the usage of WIL versus using user-authentication-based Pre-Boot Authentication according to the requirements of implemented enterprise security standards and goals.

Resizing Partitions: Never use any disk partition editing software when Full Disk Encryption is installed on the workstation.

If you need to resize a partition, remove Full Disk Encryption completely first and then resize the partition.

Overlapping Partitions: When moving disks between computers where the computers have different head counts (e.g. H=64 → H=16) FDISK may produce overlapping partitions. The operating system does not notice this. Full Disk Encryption will not start encryption if overlapping partitions are found. This problem can sometimes occur on machines with multiple volumes.

System on Volume without Drive Letter: If the system partition is not accessible using a drive letter when Full Disk Encryption 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 Full Disk Encryption is installed, doing so may lead to an unusable system.

**OS Upgrades:** Do not upgrade from one operating system version to another while Full Disk Encryption is installed, for example upgrading from Windows 2000 to Windows XP. This may lead to an unusable system. However, you can install hotfix upgrades.

**Remote Help Malfunctions on Slaved Hard Disk Drives:** Remote Help’s remote password change and one-time logon do not function on slaved hard disk drives.

**Anti-virus Software:** Full Disk Encryption is not fully compatible with some anti-virus software. The encryption process performed by Full Disk Encryption is performed in the background and does not affect computer performance noticeably. However, if anti-virus software runs a disk scan while Full Disk Encryption is encrypting the disk, performance will be impaired. Full Disk Encryption Support can provide more information on this issue.

BIOS anti-virus feature functionality should be disabled. If active, it will cause the system to hang when reloading from suspend mode.

**Full Disk Encryption and VMware:** Full Disk Encryption 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 Full Disk Encryption is severely restricted in VMware sessions.

**Full Disk Encryption and Windows Vista BitLocker Drive Encryption:** Windows Vista BitLocker Drive Encryption cannot be used together with Full Disk Encryption.

**Modifying the Pointsec for PC.msi Package Not Supported:** Do not modify the Pointsec for PC.msi package in any way. For instance, do not attempt to modify the Pointsec for PC.msi package by using transforms. Modification of the Pointsec for PC.msi package invalidates the supportability of the product.

**Unformatted Partitions Will Trigger the Cancellation of the Installation:** If computer on which Full Disk Encryption is being installed has an unformatted partition, the installation will be cancelled.

**Multiple Drivers Can Hinder Upgrade:** Having multiple drivers allocated can cause upgrade to fail. Workaround: Reduce the number of drivers to one set of a card and a reader driver before upgrading. More drivers can be allocated after the upgrade is complete.

**Smart Card Feature in the Full Disk Encryption Preboot Environment:** Systems that do not allow the disabling of USB Legacy support in the BIOS may be incompatible with the smart card feature in the Full Disk Encryption preboot environment.

**Windows Vista's ReadyBoost™ and ReadyDrive™ Are Not Supported:** Full Disk Encryption does not support the use of Windows Vista's ReadyBoost™ and ReadyDrive™ technologies. Support for these technologies will be added to a future Full Disk Encryption release.

**FIPS Compliant Dynamic Tokens Are Not Supported:** Full Disk Encryption does not support dynamic tokens that are formatted to be FIPS compliant.

**Token Insertion/Removal Handling Feature:** The Full Disk Encryption Token Insertion/Removal Handling feature is unreliable except when using Aladdin eTokens.
Known Limitations

Deployment Software: When Full Disk Encryption 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.

Alternative Boot Menu: The options displayed in the alternative boot menu depend on what the BIOS of the machine supports and the hardware that is currently installed. Therefore, the fact that an option is listed in the menu does not mean it is supported by Full Disk Encryption.

SATA USB/CD/DVD devices not supported in Alternative Boot Menu: SATA USB/CD/DVD devices are not supported in the Alternative Boot Menu.

Japanese Language Pack Does Not Contain All Japanese Characters: The Full Disk Encryption Japanese language pack does not contain all Japanese characters. This means, for example, that if the computer name contains Japanese characters that are not contained in the Japanese language pack, these characters will be displayed as black boxes.

Multiple Hard Disks: Full Disk Encryption R70 supports up to six hard disks, which together can have a maximum total of 12 volumes protected by Full Disk Encryption.

Recovery and Hibernation: Do not attempt to perform recovery on a hibernated machine.

Hidden Volumes: Full Disk Encryption 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 Full Disk Encryption Preboot Environment is loading. USB devices, bootable CD-ROMs, and bootable DVD-ROMS are not supported in the system during the Full Disk Encryption Preboot Environment and during preboot authentication.

Specific Issues - General

00417189 When creating silent installation packages on a computer with SecureClient or SecuRemote, make sure that you add the following line to the pre-check file:

(CompatibleGinas=ckpginashim.dll)

For additional information regarding the pre-check file, refer to the Full Disk Encryption Installation Guide.

00453085 HP Compaq 6910P Notebook PC experiences intermittent blue screens in preboot.

00452853 Blue screen occurs when using multiple disks. FDE can blue screen with error code 0x0500128BD if you have multiple disks in the system, especially if you have different kinds of drives (for example, IDE and SCSI, or IDE and SATA). The crash happens when the first disk that Windows discovers (and notifies FDE about) is not the boot disk.
00452500 Deleting a user account via MIMC fails to trigger the writing of a new recovery file. The following scenario will produce the problem:

1. Full Disk Encryption is installed, running, and configured.
2. Add a user account which has uninstall and recovery permissions via MIMC.
3. A new recovery file that includes the new user account is written.
4. Remove the user account via MIMC.
5. A new recovery file is not written.

**Workaround:** To trigger the creation of a new recovery file, change the password of an existing user account that has uninstall and recovery permissions.

00451763 Token removal function “Lock workstation” fails when using a SafeNet iKey 2032 USB token. Lock workstation works when the token is removed, but when it is reinserting nothing happened and the smart card error dialog displays: “An internal error occurred”.

**Environment:**
- **Middleware:** SafeNet AS470MU20
- **PC:** Lenovo T61p
- **Partition set:** 9 volumes
- **Algorithm:** Blowfish

00451753 Possible problems if HID drivers are deployed to non-tablet PC EW/MI clients. If you deploy Full Disk Encryption to non-tablet EW/MI clients, and the deployment contains HID drivers; the clients might not be able to boot into FDEPBE.

**Workaround:** Disable the HIB drivers in the double-shift menu on the non-tablet PC EW/MI clients that have experienced the problem.

00451750 Password synchronization will not work if you log on to Windows Vista using a UNC user name, for example, “maer@pmt-test.pointsec.com”.

**Workaround:** For example, log in as “maer\pmt-test.checkpoint.com” and password synchronization will function correctly.

00451701 Single sign-on (SSO) fails on Vista when using a user account name that contains an at sign ‘@’. The following scenario will produce the problem:

Enable SSO. Use a temporary password to create a user account with the use account name that contain an at sign, for example: maer@pmt-test.pointsec.com.

When Windows displays the SSO dialogs, log on as maer@pmt-test.pointsec.com in the normal Vista logon screen.

After rebooting and logging on in the FDEPBE, the Vista logon screen is displayed, then “Please Wait” is displayed, then the screen goes blank and “Please wait” is displayed again and again. It loops this way until you shut down the machine with the power button.

00451653 A 2048 bit certificate will fail on the ActivIdentity Activkey Display token. The token supports 2048 bit certificates, and you can install the certificate on the token; but when authenticating in preboot the message “Invalid logon - The token or reader driver entered an unexpected error condition” is displayed. With a 1024 bit certificate, the ActivIdentity Activkey Display token works without problems.
Full Disk Encryption-to-Windows password synchronization and Novell single sign-on (SSO) do not work together. The scenario that produces the problem is:

1. Install Novell Client 4.91 SP3.
2. Install Pointsec PC.
3. Enable “Synchronize Preboot Password to Windows” and “Enable SSO” on a user account.
4. Make sure to initially have the same password in Windows, Novell and Full Disk Encryption.
5. Establish the SSO chain between Full Disk Encryption and Novell.
6. Change Full Disk Encryption password in preboot. During logon to Novell/Windows you get the message that Windows password has been synchronized with Full Disk Encryption.
7. Reboot and logon with new password in preboot. During logon to Novell/Windows a message that SSO is enabled pops up (this is OK) but authentication halts on the Windows credentials (since it has been synchronized). Enter the new Windows password and you will logon but SSO will not re-establish. Reboot and re-enter the new Windows password several times but SSO chain will still be down.

Note: The other password synchronization feature “Synchronize Windows to Preboot Password” works with SSO.

When doing a master installation of FDE, the installation procedure requires the input of license server details. The fields cannot be "skipped" but the user will not be "nagged" by dialogs if no server has been found for the path used. So any server password and path can be entered.

How To Respond to Wizard and Sanity Check Requests for License Server Details After Installing FDE R70 EA. During a master installation the FDE R70 EA version using a non-evaluation Check Point license, the MSI.exe wizard will request that you specify a "License server folder path" and a password that will be used to access the license server. Specify a path and a password.

The PCMC will display "sanity check" warning if no "License server shared folder path" or "License server password" has been specified and a non-evaluation Check Point license is configured in Local settings or the relevant profile. You can either specify a path and a password, or you can ignore this warning.

But because no TP owner as been assigned, the description of the fix in the bug is under "Repair". Also added a cross-ref under Upgrading to the bullet for "6.x.x" pointing to the Know Issue that it is not possible to upgrade directly from 6.0.0. to FRE R70.

Creation of recovery file on a SanDisk Cruzer USB fails. When trying to create a recovery file on a SanDisk Cruzer USB and unlocking the recovery file in the two steps, the creation of the file on the USB stick will fail on a SanDisk Cruzer. This issue will occur only if the USB stick is used in standard (delivery) mode. If the onboard application is removed, and the stick formatted it should work as a normal USB stick.

If Full Disk Encryption EW/MI is installed on a Dell D830 that uses a Flash Cache module, a memory error occurs on the first reboot after installing. If the PC is turned off after the error message is displayed and then is started again, the FDEPBE code is written, and Full Disk Encryption is installed successfully. This occurs on Dell D830s with the flash cache module enabled in BIOS.
00400006 Black screen is displayed, and therefore there is no access to preboot authentication, when “Enable USB Devices in Preboot” is active and a USB smart card reader is enabled. Workaround: disable the USB smart card reader.

Environment: computer: Lenovo T61 7659-CTO, smart card: RSA SID 800.

Workaround: disable USB SmartCard reader.

00399878 Sometimes it is not possible to install Full Disk Encryption 6.3.1 on a Windows 2000 client which previously had Full Disk Encryption 6.3.1 installed and subsequently successfully decrypted and removed. This problem only occurs if the client had been upgraded first from version 5.2.3 to 6.3.0 and then to 6.3.1.

00399820 Exception occurs when upgrading from the Full Disk Encryption 6x series if a USB memory stick is inserted on Dell Inspiron 9400. The scenario that produces the error is:

1. Upgrade from Full Disk Encryption 6.2HF2 to 6.3.1 on a Dell Inspiron 9400 with Vista installed.
2. Insert a USB memory stick (in this case, a SanDisk Cruzer).
3. Reboot. An exception occurs (green screen) prior to display of the FDEPBE.
4. Press a key and the FDEPBE is displayed and normal operation proceeds. Thus the green screen occurs only once.
5. The problem also occurs when trying to upgrade from 6.1.1 to 6.3.1 on same type of PC but with Windows 2K as the OS.
6. The green screen you only get once. When the USB memory stick is removed and you boot the machine, a black screen is displayed. This can be fixed by rebooting and disabling USB legacy in the BIOS.

00396360 An intermittent issue occurs when logging on to the FDEMC using a smart or fixed password -- the log-on dialog disappears, but the PCMC window never appears. The PointsecForPC.exe process remains visible in the task manager.

Workaround: Close the process and try again.

00399654 If Windows Integrated Logon (WIL) is enabled on an MI client, and then WIL is temporarily disabled using the tray, WIL is re-enabled by any manual update sent from the MI Framework to the client.

Note: If you want to use WIL, ensure that the WIL setting in the MIMC is enabled. It is not enough to enable WIL for an end user using only the WIL switch in the FDEPBE.

00399600 If “Mouse support” is enabled in the PABM on a HP DX2000MT either the USB/PS2 Keyboard or the USB mouse works, but not both, in FDEPBE. If you disable “Mouse support”, the keyboard works. If “Mouse support” is enabled and BIOS “USB legacy support” is disabled, both the mouse and the keyboard work in FDEPBE.

00399560 After a Wake-on-LAN (WOL) logon, the number of remaining allowed WOL logons is not reported to the MI Framework. The next time an update is sent to the MI client, the number of logons allowed on the client will be erroneously reset to the original number of allowed WOL logons.
00399120 Hibernation start fails when using 3DES. The scenario that produces the error is:

1. Install Full Disk Encryption and encrypt the system volume using the 3DES algorithm.
2. Once encryption has finished, hibernate the PC.
3. Start the PC, and log on to FDEPBE.
4. Note that it says “Starting Windows” instead of “Resuming Windows” as it should. Apparently the PC can be hibernated, but it can not be restored afterwards. Unsaved documents etc. at the time of hibernation are lost.
5. Hibernation using the CAST algorithm on XP SP2 and using the AES algorithm on 2000 UR1 works fine.

Environment:
- **OS:** 2000 UR1
- **FS:** FAT32/NTFS
- **HARD DISK DRIVE/Volume:** 1/3 (First hidden)
- **Algorithm:** 3DES
- **PC:** Dell D830 and Dell D600.

00397785 Token removal handling does not function with all tested smart cards and smart card readers. Tested different settings of the token removal feature on three different PC's using two different sets of smart cards/readers. Only the token removal setting “Do nothing” worked. It seemed to work only the first time because only the first attempt was added to the logs.

This feature has been tested earlier on Windows 2003 Server and Windows Vista with Alladin eToken middleware, and was reported that it worked.

Environment info:
- **PC1:** Dell D370
- **PC2:** IBM T60
- **PC3:** Dell D620
- **OS:** Windows XP SP2 on all PC's
- **Middleware 1:** RSA authenticator 1.0B25
- **Middleware 2:** AuthentIC 3.6.2
- **Smart card 1:** RSA 5200
- **Smart card 2:** Oberthur 64 RSA v5.3

00397727 Administrators cannot use the UseRec.exe application directly on the MI server to create recovery floppy disks, etc.

Issues:

In the directory: \1_Pointsec for PC\Tools\Reco_img\6.3.0, ccore32.bin is missing. This makes it impossible to run the UseRec tool directly from, for instance, a Full Disk Encryption installation CD.

The Visual Studio 2005 runtime files are not installed with the Full Disk Encryption PC 6 module. They need to be added as merge modules in the installer in order to run UseRec.exe.

This means that the admin has to use a deployed client to create recovery media for other clients.
00395374 If the SSO chain between Full Disk Encryption and the Novell Client is established and password synchronization is performed, it will take 3 reboots to re-establish SSO. The scenario that produces the problem is:
1. Establish the SSO chain between Full Disk Encryption and Novell Client.
4. Reboot and SSO chain will be broken. It will take two additional reboots before SSO is established again.
5. Note that performing the same scenario with Windows GINA instead of Novell GINA requires only 2 reboots.

Environment info:
- **Full Disk Encryption version**: 6.1.3 build 1108
- **PC**: HP T3350
- **USB controller**: OHCI
- **OS**: XP SP2
- **FS**: NTFS
- **MSI**: Windows Installer 3.1
- **.NET**: 1.1 & 2.0
- **Novell Client**

00398150 If USB devices are attached to the Hewlett Packard d230MT, it displays a black screen, thus inhibiting display of the Full Disk Encryption PC preboot environment (FDEPBE) for authentication.

**Workaround**: Disable “Legacy USB Support” in the BIOS and ensure that the Enable USB Full Disk Encryption setting is enabled.

00397791 An ampersand (&) cannot be used in a profile name when creating a profile.

**Workaround**: Use only English upper- and lowercase characters and the digits 0-9.

00397751 When a smart card user is configured with “Use Full Disk Encryption Token Insertion / Removal Handling” enabled, and uses a DoD CAC with ActivCard Gold for DoD CAC middleware, once the system takes the setting, the removal of the smart card takes a short while to lock the system (a few minutes), but then locks the system.

If the card is inserted, the system will automatically “lock” (i.e. go to screen saver mode) after a few minutes (about 3-5 minutes), regardless of user activity, so it is not behaving like the screen saver. The screen saver setting is configured for 10 minutes, but changing that value has no effect.
**Known Limitations**

00397681 Ctrl+Alt+Delete required when logging on in Vista with SSO.

In some circumstances even though SSO is enabled in Full Disk Encryption, Vista forces the logged in user to press “Ctrl + Alt + Delete”. After pressing “Ctrl + Alt + Delete”, the user is automatically logged in.

To eliminate the “Ctrl + Alt + Delete” step, go to the Control Panel -> User Accounts. Click “Manage User Accounts” and click the “Advanced” tab. To eliminate the need to press “Ctrl + Alt + Delete”, clear the “Require users to press Ctrl + Alt + Delete” check box.

00397427 Full Disk Encryption 6.2 contains an Automatic upgrade function. This function is used to perform upgrade by distributing an Upgrade package to the “Upgrade path” or the “Work folder”. In Windows 2000 and Windows XP, the end user is notified of the progress of the Automatic upgrade and is notified when the upgrade has been finalized. In Vista the upgrade does not display this information.

00397231 The PME setting “Use SSO with P4PC” works only when Full Disk Encryption is installed before PME.

00397223 The FDEPBE hangs if a docking station is attached to the PC Acer TM 4400 and USB is enabled. If USB is disabled, the FDEPBE does not hang. However, in this latter case, the keyboard and mouse attached to the docking station do not work.

**Workaround:** Disable USB support in FDEPBE via the FDEMC setting “Enable USB”.

00396962 Cannot perform SSO with Entrust smart card user. The reason for this is that an error occurs when an attempt is made to store an Entrust profile required for SSO, on the smart card.

00396807 The Windows driver (prot_2k.sys) crashes if the system contains only 4.x/5.x volumes. This situation may occur if an upgrade is aborted in the FDEPBE and recovery is not performed on all volumes. The situation can be fixed by performing recovery on all volumes.

00396793 A user account with password authentication and the setting Case sensitivity = No or Convert to uppercase in 4.x/5.x = Yes may experience trouble providing Remote Help if he/she has not entered the password in uppercase letters.

**Workaround:** Request that the person providing Remote Help use capital letters when entering the password in his/her system.

00396024 The installation of Full Disk Encryption is stopped if the Proventia Desktop version 8 or 9 is installed. There are two possible workarounds for this issue:

Disable the Proventia Desktop during installation of Pointsec PC.

Add prot_ins.sys to Proventia Desktop exclusion list during installation.

00395865 No FDEPBE logon screen is displayed if an eToken NG Flash USB smart card is used on a Dell Inspiron 9400. After PC boot, the screen goes black and the FDEPBE screen is displayed.

**Workaround:** Set the BIOS setting “USB Emulation” under POST behavior to “OFF” to avoid the problem.
If the single sign-on (SSO) chain between Full Disk Encryption and a Novell Client is established and the following password synchronization scenario occurs, it will take three reboots to re-establish SSO. Here is the scenario:

1. Establish the SSO chain between Full Disk Encryption and a Novell Client.
2. Activate password synchronization with Windows.
3. Change the password in Novell/Windows.
4. Reboot and the SSO chain will be broken. It will take two additional reboots before SSO is established again.

The same scenario with Windows GINA instead of Novell GINA requires only two reboots.

While deselecting volumes one of the volumes suddenly disappeared from the list. The “lost volume” reappears after any key is pressed.

Due to architectural difference between Full Disk Encryption and Computrace software, there is compatibility issue between Full Disk Encryption and Computrace software when Computrace is run in software persistence mode.

Workaround: Rewriting the master boot record makes the machine boot normally, for example, fdisk /mbr.

Interoperability problem with PME and recovery media creation. When creating recovery media to a USB memory stick while having PME installed, there may be a problem after the first part of the creation is done.

After unplugging and re-inserting the USB memory as instructed by the program, a blank (all white) PME window will sometimes pop up after you have pressed OK. Both windows (PME and Full Disk Encryption recovery media) will stop responding, and you will have to close the applications via the Task Manager.

When ordering a restore from within the Windows part of RRU, the computer restarts and then boots into RRU before allowing you to authenticate in FDEPBE. If you reboot from within RRU, you will get to FDEPBE; and then you will boot into RRU and it will perform the requested restoration.

You can experience difficulties when creating an installation profile that is based on local settings when you are required to provide new authentication for the profile and you want to use a smart card you have used previously. In this case, Full Disk Encryption requires that you re-associate the smart card (plus certificate) and the user; and this it may not always be possible to acquire all the certificates needed for all the users.

Workaround: Rather than trying to re-assign the smart card to the user, assign the user a fixed password and switch to smart card and certificate later. Alternatively, define a temporary smart card user so the user can reassign the certificate him/herself on the next boot of the PC.

Do not remove the PCMCIA reader or smart card while authenticating. They can be removed when authentication has been completed in FDEPBE.

When single sign-on is enabled, if you change your password in Windows, single sign-on will be temporarily disabled. The next time you log on, a message will be displayed saying that Full Disk Encryption cannot log on to Windows - please enter your Windows password. After you correctly enter your Windows password, single sign-on will again function.
The following password rules conflict with full Unicode support:

“Require letters and integers”.

“Allow Special Characters”. The current description in the FDEMC of this setting is: “Besides a-z, A-Z and 0-9, allow the use of the semicolon and the following other special characters: ! "$ % & ' ( ) * + , - . / : < = > ? @ { }”. As described, the setting would not allow the full range of Unicode characters to be used whether set to “On” or “Off”. With regards to actual Full Disk Encryption functionality, the following is a more accurate description: “Allow use of the following special characters: ; ! "$ % & ' ( ) * + , - . / : < = > ? @ { }.” If this setting is set to “No”, these special characters are not allowed in passwords. However, all other Unicode characters are allowed regardless of the setting.

“Require upper and lower case”. This only makes sense in alphabets that have case forms.

“Allow password of adjoining characters.” This is meant to prevent entering series of characters from adjoining keys on the keyboard. However, only western-style keyboard layouts are used to detect adjoining characters.

The RRUinstall.msi installer installs the driver required by Full Disk Encryption to support RRU, on the wrong volume.

Workaround: specify the target drive with the MSI Property TARGETDIR=C:\. For example: msiexec /i InstallRRU.msi TARGETDIR=C:

If you lose mouse functionality when running the recovery program individual volumes cannot be selected.

Workaround: Recover all volumes rather than selected volumes.

**Specific Issues - Hardware**

No support for hybrid disk. If ‘NV cache’ is enabled, the installation will fail to install. The Full Disk Encryption SA seems to be written on a cache part. So the SA seems to be flushed and the installation fails. Disable NV cache and install Full Disk Encryption, then enable NV cache gives database corrupt randomly in preboot.

Environment info:
- Znote 6224w
- Vista Ultimate
- HARD DISK DRIVE: Samsung HM16HJI ATA Hybrid Hard Disk

The combination of an Axalto Cyberflex Access 64K Pegasus v2c smart card and a Schlumberger USB Reflex Version 1. smart card reader fails in preboot. Preboot authentication using the combination of an Axalto Cyberflex Access 64K Pegasus v2c smart card and a Schlumberger USB Reflex Ver 1. smart card reader fails.

Connecting a Dell D410 to a Dell external USB bay can prevent the machine from booting into FDEPBE. If the bay is connected in FDEPBE, the machine can terminate with a black screen immediately after FDEPBE logon. Both behaviors are intermittent, and both occurred when a CD-ROM (with no CD) was connected to the bay.
00395744 Using a smart card on an MCP ClientPro 365 machine with the following BIOS settings, will cause the cursor to blink:

- plug and play os = no
- legacy usb = disabled

Workaround:
- Use the factory BIOS settings, which are:
  - plug and play os = yes
  - legacy usb = enabled.

00395492 The FDEPBE authentication window freezes when both a smart card reader and an Iomega USB BXXU0130 floppy disk drive are attached to the machine. Removing the Iomega USB floppy disk drive will activate the FDEPBE authentication window again, and you can proceed. This problem has occurred on the following PCs: Dell Inspiron 9400, Dell Latitude D600, Sony Vaio Z1.

00395395 Logon in Windows environment with the Setec EID IP2 smart card will crash the FDEMC tray because of problems with the CSP.

00395265 The USB mouse does not work in FDEPBE on the Acer Ferrari 3200. The optical USB mouse has its light on in the BIOS, the operating system, and in the Full Disk Encryption alternative boot menu; but not in the FDEPBE.

00395086 Hot plugging of USB devices does not work on the IBM-Lenovo ThinkPad T60. You can log on with a USB token if it is plugged in from start.

00395036 The FDEMC crashes when trying to read the certificates stored on smart card “Setec EID IP2”. The FDEPBE does not recognize any certificates stored on smart card “Setec EID IP2” when using smart card reader: CardMan 4040 (PCMCIA) together with the following drivers: cm4040.bin and opensc.bin.

Workaround: Copy the certificate to Windows the personal store using smart card middleware.

00394747 Not possible to log on in FDEPBE with RSA SID 800 and Ferrari 3200. The following scenario produces the problem:

1. Install Full Disk Encryption using an interactive profile with one smart card account. The files: msc_p11.bin and prd_ccid were added to precheck.txt.
2. Middleware was installed after installation of Pointsec for PC.
3. After reboot, with the smart card inserted, no pin code dialog box is displayed in the FDEPBE. Nor is the pin code dialog box displayed when the smart card is inserted after reboot but before logging in to FDEPBE.

This problem concerns RSA SID 800 and Ferrari 3200.

00394678 The USB hub Targus PAUH210 does not work with the HP T3350 in the FDEPBE (the Full Disk Encryption preboot environment).
00394617 When USB smart card support is enabled, and no FDEPBE smart card drivers are installed, the HP T3350 desktop PC may hang before the FDEPBE authentication is displayed.

Workaround: Specify the following BIOS settings:
- PNP operating system should be set to YES
- USB legacy support should be set to ON
- Note that the above settings are the factory settings.

00394606 On a Fujitsu Siemens 7020, a USB mouse/keyboard will not work in FDEPBE if they are connected via a Targus PAUH210 hub. USB mouse and keyboards did work when connected via other hubs.

00394595 When USB media is used to perform recovery on the IBM A51, an error occurs when you boot into the recovery program. The error message is as follows:

Divide error
***Program terminated, rc=03***

This seems to have to do with the startup device menu, where the USB media must come before the Hard disk drives instead of after them.

Workaround: It is possible to perform recovery with USB media if you ensure that the USB device comes before the hard disk drives in the startup device menu.

00394487 Unable to use the keyboard in the preboot customization menu after USB smart card support has been enabled on an ACER TM 4401 notebook. The keyboard does not function in the FDEPBE either, so you cannot logon. The problem does not occur on each reboot. It appears more frequently when other USB devices are connected or used or both during preboot.

00394471 Wrong smart card driver for smart cards with identical ATR string in FDEPBE. In the FDEPBE, smart cards are handled via loadable drivers. The driver that is used for a specific smart card is set up via registry (.inf) files. The registry files may contain one or more smart card entries.

Each entry consists of the smart card ATR string and the name of the FDEPBE driver that will be used for the smart card. Unfortunately, several smart cards may use the same ATR string, and therefore the same ATR string may be present in several entries, which each identify a different driver. When a smart card is detected in the FDEPBE, the ATR string is extracted. The first driver, according to the registry file, that is available in the FDEPBE is thereafter loaded and used to handle the smart card.

This means that if several smart card drivers which support the same ATR string are available in the FDEPBE, the wrong driver may be used. To minimize the probability of this happening, the number of smart card drivers in the FDEPBE should be minimized.

00394188 If a SanDisk CompactFlash® PC Card Adapter is present at preboot authentication, a fatal error occurs with error code 0x50010DA during Windows boot. This occurs even if PCMCIA support is disabled in preboot.

00394177 An RSA SecurID dynamic token is not detected on an Acer Ferrari 3200, a Dell Inspiron 6400, and a Dell P670 when inserted in FDEPBE.

Workaround: Insert the RSA SecurID dynamic token before you turn on the PC.
On certain machines, Full Disk Encryption does not detect the presence of a smart card token, for example, an RSA SecurID 800 authenticator, and does not display the PIN dialog in the preboot environment. This can happen in the following two scenarios:

**Scenario one:**
The machine is on and the preboot logon dialog is displayed.
Insert the smart card token, but no PIN dialog is displayed.

**Workaround:** With the smart card token still inserted, turn the power off and wait a few seconds. Then turn the power on while the smart card token is still inserted, and the PIN dialog will be displayed.

**Scenario two:**
Insert the smart card token and turn the machine on. The preboot logon dialog is displayed, but the PIN dialog is not displayed.

**Workaround:** Remove the smart card token, turn the power off, and wait a few seconds. Turn the machine on again. The Full Disk Encryption preboot logon dialog is displayed. Insert the token and the PIN dialog will be displayed.

eTokens do not function on Acer Ferrari 3200 PCs.

**Specific Issues - Documentation**
Cosmetic errors exist in the documentation: some screen images can be “back-level” and/or do not match the text. Note that the text is correct; it is the screen captures that are back level.

The following is late-breaking documentation which will be added to the relevant guide as soon as possible:

The next version of the *SmartCenter for Pointsec - MI Full Disk Encryption Module Installation Guide* will mention the name of the folder where the Full Disk Encryption 6 files are stored: “PPC6 MI Client”. The files in this folder are used when creating a local copy manually from the installation CD.

The next version of the *SmartCenter for Pointsec - MI Full Disk Encryption Module Installation Guide* will clarify that you should not upgrade Full Disk Encryption on a client while encryption is in progress. (In this version of the management console, there is no information in the software as to why the upgrade fails if encryption is in process.)
Media Encryption

Media Encryption supports the initial Vista release, but does not support SP1.

00435508 When encrypting NTFS files on a removable device, Media Encryption creates a container in FAT32 format. Because FAT32 format is limited to less than four gigabytes, any file larger than 4Gb cannot reside inside the container and therefore will not be encrypted.

00408539 When encrypting a CD or DVD, a Windows CD window may appear. You can safely close and ignore this window.

00408639 When running the Deployment Utility from the CD on a computer that is already running Media Encryption or Pointsec Protector, the ME/Protector profile must allow executing programs from CD. Otherwise Media Encryption/Protector will prevent running the installation.

00410839 The Removable Media Manager options on the Media Encryption page are unavailable after inserting a USB device.
   Workaround: Refresh the screen or select another option on the page. The Removable media options now appear as available.

00413147 Windows Server 2003 is not supported.

00413148 In the current version, the Deployment Utility does not perform any security validations on installers and packages. Please ensure that these items originate from a trusted source.

00419844 The Read Only configuration option is not supported for removable media and CD or DVD devices on Windows Vista.

00417056 Users may unable to create or modify custom profiles or users in Full Disk Encryption.
   Workaround: When creating a custom profile, click on another tab and make an irrelevant change. Click Apply. The custom profile will now be successfully updated.

00420269 Rebooting a client computer before the installation process completes successfully may cause the computer to fail to restart. Backup all client computer data before starting the installation process to avoid data loss.

00452643 Media Encryption can encrypt an external hard disk only with a single partition (primary or extended).
   If encryption of an external hard disk fails to complete successfully, perform the following troubleshooting steps.
   1. Open the Windows Control Panel.
   2. Select Administrative Tools > Computer Management (Local).
   3. Select Disk Management in the Console Tree.
   4. Locate your external disk and verify that it has only one partition.
   5. If your external disk has more than one partition, you must perform the following steps:
      a. Back up the data and re-format the disk as a single partition (primary or extended).
b. Restore the backed up data to the newly formatted disk.

c. Encrypt the newly formatted disk using Media Encryption.

**Secure Access**

Secure Access does not support Microsoft Vista.

00409112 Using the FORCEREBOOT custom parameter in the Secure Access package with the deployment utility can cause undesirable results. Do not use the FORCEREBOOT custom parameter as this will force a reboot of the target system prior to the entire Endpoint Security installation finishing.

00223454 Sometimes the Antivirus/Antispyware panel will fail to load with the message "The Anti-virus / Anti-spyware panel failed to initialize. The resources for the panel may be missing or corrupt". Restart the client to load the Antivirus/Antispyware panel.

00223819 The kernel portion of the Antispyware engine for the Endpoint Security client does not install on endpoint computers running the Windows 2003 Server operating system. This results in a reduction in the protection and treatment of certain malware with kernel mode components.

00223936 The documentation regarding Program Control behavior in the disconnected policy is incomplete. It should contain the following information:

By default, program group permissions are not included in the disconnected policy. If a client is using the disconnected policy and the program is not governed by Program Advisor permissions (because Program Advisor is not enabled or the client is not allowed to ask Program Advisor directly for the permissions) the program will receive the permissions you have set for Unrecognized Programs.

In this release, you can include program group permissions in your disconnected policies by selecting the Group Settings Available in the Disconnected Policy option on the Program Group Page. Note that including group permissions can substantially increase the size of your policy. Including too many groups in your policies may make your policies too large and cause performance issues.

If you are using disconnected policies, it is recommended that you create a group that contains the most essential programs for your organization and select the Group Settings Available in the Disconnected Policy option for that group. It is also recommended that you allow the client to contact the Program Advisor Server directly. This will ensure that your users always have access to the most important programs.

00223948 The documentation is missing information on the disable wireless on LAN feature. Use the following instructions for this feature:

You can use the Disable Wireless on LAN feature to prevent your endpoint users from being connected to an unauthorized wireless network while using your LAN. This helps to protect your network from threats that your endpoint users may acquire from the wireless network.

To disable wireless while on the LAN

1. Go to the Client Settings tab in the policy.
2. Select the Disable wireless adaptors when connected to LAN option.
3. Click Save.

**00413532** When upgrading from version 7.0.843.000 and experiencing the certificate issue described in Secure Knowledge Article SK34878, the upgrade will sometimes cause the endpoint computer to become unresponsive. If this happens, restart the endpoint computer and subsequent upgrades will succeed.

**00419341** In some circumstances on Windows XP, Endpoint Security will cause frequent reboots. This is due to an issue within the operating system. The following hotfix from Microsoft is available for this issue:

http://support.microsoft.com/kb/936456

Install this hotfix or upgrade to Service Pack 3 to solve this issue.

**License Server and Reporting Tool**

The User Center supports a single license file containing all Endpoint Security licenses. When such a file is added to the License Server, warnings may appear in the log file regarding missing features in the cp. macro file. For example, the following may appear: "Warning: Can't find: CPIS-ISPY-5-NGX in cp.macro. License version might be not compatible". These warnings can be safely ignored.

The License Server does not support license files that contain more than one license, except for the single license file that contains all Endpoint Security licenses.
Resolved Limitations

This section presents details of limitations that were resolved in previous releases.

In This Section

- Full Disk Encryption
- Secure Access

Full Disk Encryption

00452256 Upgrade from Full Disk Encryption 5.x to 6.2 HFA1 freezes prior to completion. The following scenario will produce the problem:

1. Before applying the upgrade package, make sure that HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon "GinaDLL" is set to something other than pssogina.dll, for example, msgina.dll
2. Start the upgrade from Full Disk Encryption 5.x to 6.2 HFA1 (set UpdateSSO=0 in precheck.txt in the 6.2 package).
3. During upgrade, Full Disk Encryption will freeze.

Customer environment:
- Full Disk Encryption 5.x
- McAfee HIP (Host Intrusion Prevention). McAfee suite to prevent access to McAfee registry keys.

00452232 When the PC is set to English Canada language, you are not able to use some of the special characters in preboot. If you try to type them, it will not show the character you are typing. The following characters do not work {}<>=?@.

If you use the Virtual keyboard with the en-CA setting, (English Canada) instead of a physical keyboard, the following characters are available and can be used ",/<>=?.

The same issues are found when using DE-AU (German Austrian) keyboards.

00452198 Password history is case insensitive. Environment: The 'Password History' setting is set to greater than 1, and password is set to be case sensitive.

When the user changes the password to something which is only a change of case from the previous password (for example, 'passWORD' => 'PASSword'), it is not accepted. It seems to be recognized as an existing password in the password history. However password is set to be case sensitive so it should be treated as a brand new password.

The following text has been added to the Administrator's Guide: Full Disk Encryption's Password History function does not consider case sensitivity when assessing password uniqueness. Thus, if you change a password that is recorded in Password History by changing only the case of one or more of its letters, it will not be accepted as unique, and therefore that altered password will not be allowed.

00452191 The customer name is erroneously found in a Full Disk Encryption token driver file, PTD.INF.

00452173 When installing Full Disk Encryption 6.3.1 on a Dell XT Tablet, the installation stalls when installing the system code.
Resolved Limitations

00452163 Invalid Profile causes exceptions in FDEMC. The following scenario will produce the problem:

- Install version 6.3.1 with a profile that has an erroneous “Set Max Failed Logons” value.
- In Windows, start FDEMC and go to Local.
- You will receive an error.
- Press OK and you will get access to the Local settings but both buttons on bottom right are blank.

00452011 Data in DRAM actually fades out gradually over a period of seconds to minutes after the system shuts down. This enables an attacker to read the full contents of memory by cutting off power and then rebooting into a malicious operating system. When the memory content has been dumped, it can be analyzed, and by using a known algorithm it is possible to find the expanded partition key in memory. When a probable key is found, it could be used to try to decrypt a sector from the encrypted disk, and since this can be automated with a tool, there is a high risk that the correct encryption key can be found.

00451958 When the system boots (from scratch or from hibernation), the driver may be interacting with memory which is not within the driver's scope. This can cause unexpected behavior such as a stop error (BSOD).

00451815 SideBySide errors appear in the event viewer during Full Disk Encryption installation. They are caused by a Microsoft Visual Studio Manifest bug.

Workaround: install the latest Visual Studio Service Pack on the client machine before installing Full Disk Encryption.

00451555 If USB is enabled in Full Disk Encryption, the computer will hang after the Full Disk Encryption progress bar is displayed.

If USB is enabled in Full Disk Encryption, the computer will hang after Full Disk Encryption progress bar is displayed. Even if USB legacy support is disabled in the BIOS, it will still hang with a black screen after the Full Disk Encryption progress bar is displayed.

The following scenario will produce the problem:

1. Install Full Disk Encryption 6.2 HFA1 with smart card drivers (set USB to Yes).
2. Reboot, then get the Full Disk Encryption system code installation, then do a second reboot.
3. The progress bar will appear and load.
4. After it is loaded, it will halt with a black screen.

Environment:
- Toshiba Tecra M9, but the problem has also been reported on other Toshiba models such as the A200 and the A8.
- Full Disk Encryption 6.2 HFA1
Resolved Limitations

00451499 If the name of a Remote Help (RH) helper account is identical to one of the group names, the challenge code becomes <invalid>.

**Example 1:**
- System Group: SYSTEM
- User account 1: SYSTEM (helper account)
- User account 2: ADMIN
- User Group: USER
- Result: User account 1: CPFDE (RH recipient) --> challenge code becomes <invalid>

**Example 2:**
- System Group:S SYSTEM
- User account 1: USER (helper account)
- User account 2: ADMIN
- User Group: USER
- Result: User account 1: CPFDE (RH recipient) --> challenge code becomes <invalid>

**Note:** This problem occurs only when the group name is all in uppercase. If the group name is “System” or “User”, RH works.

00451427 It is possible to create two (or more) users with the same GUID when creating profiles. This is now prevented in the “sanity check” dialog prior to writing the profile to disk.

00399981 Credential change smart card to password is not updated to other clients.

1. The scenario that produces the error is:
2. From the MI Framework, deploy the same smart card user account to at least two MI mode clients.
3. Via the tray, change a user account's authentication method from smart card to password on one of the clients.
4. Wait for the MIMC Server log to refresh. You will soon get a “failed: another authentication method” log entry and the authentication method will still be set to smart card in MIMC. But, in spite of the message, the authentication method has been changed to password on this client.
5. If the user account logs on to the second MI mode client it will not have receive the credential change update.
6. The result is that you now have the user account on one client using password authentication and on the other client the same user account uses smart card authentication.

**Note:** Changing credentials via the tray from password to smart card works correctly.

A consequence of this issue is that the next time an update is sent to the first client, the update will set the authentication method back to 'smart card'.
Resolved Limitations

00399939 ActivIdentity ActivKey V2 is not recognized in PBA. The following scenario will produce the problem:
1. Install the elements listed below, and ensure that the smart card is recognized in Windows and in Full Disk Encryption.
2. Define a smart card user account and choose the certificate.
3. Reboot with the smart card inserted.
4. There is no PIN dialog; the smart card does not work in PBA.

Environment:
- XPSP2
- ActivClient_5.4_bn457
- ActivIdentity Device Installer 2.1 x86 (BN 12)
- Full Disk Encryption 6.2.0 HFA1 (1226)
- Smart card:
  - ActivIdentity ActivKey V2
  - Axalto Cyberflex Access 64K V1 SM 2.1
- Full Disk Encryption drivers installed:
  - Ac_p11.bin
  - ActivKey.bin

00399936 Recovery file not written after resetting the value of the 'Logon authorized' setting. After setting 'Logon Authorized' to 'No' for a user account, a new recovery file is written. But if you then change this setting by right clicking and selecting 'Reset value' so that you once again inherit the value (in this case YES) from the group, a new recovery file is not written. If you however set the value to YES you will get a new recovery file. Resetting the value does not seem to trigger the writing of a new recovery file even though the value has changed from 'No' to 'Yes'.

00399894 The sanity check which appears when closing FDEMC warns that fewer than two user accounts have permission to perform uninstall in the following scenario:
1. For the System group, specify the settings “Uninstall” and “Create recovery media” to: No.
2. On two user accounts in the System group, set “Uninstall” and “Create recovery media” to: Yes.
3. According to the new inheritance rules, the user account settings should override the group settings.
4. Close FDEMC, and a Sanity check will be displayed warning that fewer than two user accounts have permission to perform uninstall.

00399872 If you add new additional recovery paths after installation, new recovery files should be written to the directories addressed by the new paths. Three new paths were added after installation but recovery files were not written to the paths. Neither logging on to Windows several times nor running crerec.exe manually resolved the problem. The recovery file was written only after changing a value that triggers a recovery file update.
Some settings cannot be reset once they have been set. For example, if you change the setting Enable SSO to “YES” on a user account and deploy the profile, the client accepts the profile and the user account can log on using SSO. Then you reset the value in the framework and deploy the profile to the clients but the value is still set to “YES” and can log in using SSO even though the local log in FDEMC also says that the configuration of the profile has been made. This also applies to the “Password Synchronization” and “Single Sign-On” settings.

When providing Remote Help from FDEMC and navigating with the keyboard and Tab key (the mouse is not used) you got an error message with code 1280. The scenario that produces the error is:

Open the FDEMC.
1. Go to Remote Help.
2. Enter the End user account name and Helper account name.
3. Select Dynamic token in the Type of helper authentication field.
4. Use the keyboard and tab to generate the response.
5. Press Enter.
6. Error with code 1280 is displayed.

The “Smart Card Triggers Windows SSO logon” setting does not work. Enabling the setting should trigger SSO for the smart card user account, but it does not.

The following scenario will produce the problem:
1. Install Full Disk Encryption 6.2 HFA1.
2. Create a smart card account and confirm that it works.
3. Enable the “Smart Card Triggers Windows SSO logon” setting for the smart card user account.
4. Reboot the machine. When logging on to Windows, the user will be asked to enter account/password. SSO does not work.

Characters in Path (recovery path/upgrade path, etc) will not be shown correctly when it contains Japanese characters. If you set a path (e.g. recovery path) that contains Japanese character, it will not be shown correctly in FDEMC.

The scenario that produces the error is:
1. Set recovery path containing Japanese character in the path (Please see screen shot JP1.JPG)
2. Close FDEMC
3. Re-open FDEMC. Check the recovery path. The path does not show correctly.

Upgrade from 4.x/5.x is normally performed via the 4.x/5.x upgrade functionality. In this case the upgrade is triggered by storing an upgrade package in the work folder/software update folder on an installation.

It should not be possible to perform an upgrade by executing the Full Disk Encryption MSI package (which is part of upgrade packages) manually. When this is done on a 5.x installation, the upgrade is aborted with an MSI error dialogue. However, on a 4.x installation the upgrade progresses quite far (at least if an upgrade profile is available), for example, the upgrade fails during the recovery file handling.
Resolved Limitations

00399058 After upgrading, the CreRec.exe fails upon start of the tray application. The scenario that produces the problem is:

1. Install Full Disk Encryption 6.0.0
2. Upgrade to Full Disk Encryption HFA1
3. A few seconds after the first start of the Full Disk Encryption tray application after the upgrade, CreRec.exe fails with the following message: “CreRec.exe has generated errors and will be closed by Windows...”. After a minute or two, the error message disappears. The error can be reproduced by logging off and on again.
4. If CreRec is run manually, the error message isn't displayed any more.

00398321 When unencrypted clear-text files are present, one or more instances of the following message are written to the Full Disk Encryption MI module log (ps_pc63_dsm.log): “Log error reported from PPC. Please remove any remaining clear-text install/upgrade logs from the Pointsec PC.”

**Workaround:** Navigate to the directory specified in the Full Disk Encryption registry under Users Location. Remove any unencrypted clear-text log files from that directory.

00398155 When “Legacy USB Support” is active in the BIOS on a Hewlett Packard Compaq dc7700 Small Form Factor PC, USB keyboards do not work.

**Workaround:** Either disable USB Legacy Support in the BIOS, or use a PS/2 keyboard, or connect a USB keyboard and a PS/2 keyboard (and both will work).

00398122 When SSO is disabled and then enabled again, a 'Record New Credentials' dialog box should be displayed. But under Windows Vista it is not displayed.

The following scenario will produce the problem:

1. Install P4PC 6.2 on Windows Vista.
2. Enable SSO for a user account.
3. Restart the PC, and login as the user account with SSO box selected.
4. At Windows startup, the SSO welcome screen is displayed.
5. After logging onto Windows, restart the PC.
6. Login at PBA as the same user, account but this time with the SSO box cleared.
7. After logging into Windows, restart the PC.
8. Login as the same user account, selecting the SSO check box again to re-enable SSO.
9. The 'Record New Credentials' dialog box should be displayed, but it is not. The- user account is logged onto Windows directly.

00397774 Clearing System Settings when creating a profile based on another profile or on local settings creates an installation that fails. Create a profile (e.g. upgrade) and base it on an Upgrade profile and clear the System Settings check box when creating it. All System settings are blank in the new profile. When using this profile, Pointsec upgrades; but the installation crashes when a user tries to use any of the System Settings.

**Workaround:** When making an upgrade profile, make sure to include all settings if it's based on another profile or on the local installation's settings. Do not clear any of the 'Base on' check boxes.
00397689 Under Windows XP and Vista, if, for example, you install the Europe1 language pack and then realize that you wanted Europe2; you will not be able to install the Windows part of the Europe2 pack. When running the command shell as an administrator, you run the psccontrol command “install-win-language” and it fails with the error message “Cannot create the file when that file already exist”

Workaround: Remove the existing plang32. file from C:/Program files/Pointsec/Pointsec for PC/ and from C:/Windows/System32/, and run the command again.

00397569 The Full Disk Encryption Token Insertion/Removal handling does not work with RSA SmartCards. The problem is due to incompatibilities with the RSA middleware used to access the RSA smart cards.

Workaround: Utilize similar Token Insertion/Removal handling in RSA middleware.

00397223 The FDEPBE hangs if a docking station is attached to the PC Acer TM 4400 and USB is enabled. If USB is disabled, the FDEPBE does not hang. However, in this latter case, the keyboard and mouse attached to the docking station do not work.

Workaround: Disable USB support in FDEPBE via the FDEMC setting “Enable USB”.

00396641 When disabling WIL via the tray menu, the message “Access to your user account failed” is displayed. This message is incorrect; the message should request the user to log off.

00396452 Lenovo model T43 may fail to boot after displaying the text “Full Disk Encryption... loading operating system”. The failure results in a blank screen. This occurs only if you have a USB storage device attached to the machine and smart cards are enabled.

Workaround if this problem occurs: Remove the USB storage device and reboot the system; the machine should now boot normally.

Workarounds to avoid this problem: The following three workarounds will enable you to avoid the problem:

1. Detach the USB storage device during the boot sequence. Once the operating system is loaded, the USB device can be attached again.

2. If smart cards are not used for Full Disk Encryption preboot authentication, disable USB via the FDEMC under System Settings/Hardware Devices/USB.

3. Disable USB Legacy Support in the BIOS.

Note: This issue depends on both the hardware and the BIOS, and it is currently being investigated by Check Point.

00395668 Hibernation should not be allowed to start during an upgrade, but Full Disk Encryption does not inhibit it.

Workaround: Disable hibernation during upgrade.

00395629 If you upgrade directly from Full Disk Encryption 6.0.0 to 6.1.3, the system, local, and remote logs will be unreadable.

Workaround: Upgrade from 6.0.0 to 6.0.1 first, then upgrade from 6.0.1 to 6.1.3, and the logs will be readable.
00395332 When creating a recovery file with a USB memory stick on Acer TM4401 the mouse does not work. When the recovery menu is displayed, neither the keyboard nor the mouse works for the first 2-3 minutes. After this delay, it is possible to use keys and to tab but it is not possible to select volumes to recover -- you have to select all volumes.

00395257 If setting for USB is enabled in FDEMC (under Hardware) and a keyboard with built in smart card reader is used, the following behavior occurs in the FDEPBE: when entering the user account name, the first character is not registered or visible. For example, if the user account name is ADMIN you must enter AADMIN for it to be interpreted as ADMIN. Tested on Hewlett Packard T3350 and T3350-2.

00394826 Note that when upgrading from 6.0.0 or 6.0.1 to 6.1, the values of Access to Local setting and Access to Remote setting are, by default, set to “Yes”. These settings can of course be set to “No” after installation.

Workaround: Deploy a profile where you set this permission to “No” for your end-users as soon as you have successfully upgraded your clients.

00394776 The USB keyboard intermittently stops functioning in FDEPBE on a Hewlett Packard T3350. This happens in the following environment:
- USB mouse was connected and worked flawlessly in FDEPBE
- USB was enabled in FDEMC
- USB legacy support was enabled in BIOS
- Plug n Play OS was disabled in BIOS

Workaround: Unplug the keyboard in FDEPBE and then plug it in again.

00394609 The recovery program can fail when creating a recovery medium on certain USB devices. For example, the recovery program failed when using a USB memory stick on an IBM x60s machine, but it ran successfully on the same machine using a USB floppy disk.

Workaround: BIOS upgrade to 2.10 resolves this issue.

00393966 Booting from a USB memory stick recovery medium created by the create recovery program fails on the HP dx5150. The machine hangs after you have entered your user account name and password.

Workaround: Using a floppy disk in a floppy disk drive connected via the USB port.

00393098 Users can encounter problems when attempting to open a file by double clicking it.

Workaround: Start the recovery program, and open the recovery file there.
00380812 When viewing logs in management console (FDEMC), the logs are incorrectly an hour behind the correct time. But if the logs are exported to a CSV file they are correct.

00397774 Clearing System Settings when creating a profile based on another profile or on local settings creates an installation that fails.

Create a profile (e.g. upgrade) and base it on an Upgrade profile and clear the System Settings check box when creating it. All System settings are blank in the new profile.

When using this profile, Full Disk Encryption upgrades; but the installation crashes when a user tries to use any of the System Settings.

**Workaround:** When making an upgrade profile, make sure to include all settings if it's based on another profile or on the local installation's settings. Do not clear any of the 'Base on' check boxes.
Secure Access

In This Section

- Server Installation, Upgrade, and Backward Compatibility
- Client Installation, Upgrade, and Backward Compatibility
- Integration
- Logging, Alerts, and Errors
- Localization and Special Characters
- Gateways and Third Party Product Integrations
- Miscellaneous
- VPN
- Version 7.0 HFA 01 Resolved Issues

Server Installation, Upgrade, and Backward Compatibility

00192556 By default, Endpoint Security Distribution Utility and the Check Point SecurePlatform administration interface both use port 443 for SSL communication. If you plan to run Endpoint Security Distribution Utility on SecurePlatform, change the SecurePlatform SSL to a different port during the operating system installation. Do not change the Endpoint Security Distribution Utility default port, as this is not supported.

00204868 Normally, after installing the Endpoint Security Distribution Utility, answering “Y” to the message “Would you like to start Endpoint Security Distribution Utility after exiting?” starts Endpoint Security Distribution Utility. If this does not work, type `cpstop` and `cpstart` (or, with Provider-1 setup, type `mdsstopp` and `mdsstart`) to successfully start Endpoint Security Distribution Utility.

00208493 Endpoint Security Distribution Utility 7.0 is now certified to support 20,000 concurrent endpoint users with default configuration. Higher performance figures are possible with customization for your environment. Contact Check Point Professional Services for information about configuration for more than 20,000 concurrent endpoint users.

0022872 After installing a distributed Endpoint Security server (with a remote Smart Center), configuring the SIC communication, and installing the database, you must restart the Endpoint Security server machine in order to complete the configuration.

00374651 After upgrading an Endpoint Security server version 6.5.x to version 7.x, the Smart Portal IP and port will not be correctly configured.

To configure:

1. Log into the Endpoint Security server.
2. Go to System Configuration I Server Settings.
3. Click the Edit button.
4. Enter the correct Endpoint Server IP address and port for Smart Portal (default Smart Portal port is 4433. For example: 209.87.213.90:4433).
5. Click Save.
00374929 When installing Endpoint Security Distribution Utility in conjunction with other products from the wrapper on Linux and SPLAT, the Endpoint Security server is not configured properly until you run Smart Dashboard and install the database on the local machine.

00375433 Due to an issue in the SmartCenter import/export mechanism (existing in SmartCenter R65, and, possibly previous versions as well), when exporting and then importing a SmartCenter configuration in environments where the Endpoint Security server is managed by the SmartCenter, the communication between SmartCenter and the Endpoint Security server will cease functioning.

Workaround: Run the command `cpprod_util SetCertPath ($CPDIR)/conf/sic_cert.p12` using the value of `$CPDIR`. You can verify this (on Linux or SPLAT) by using `ckp_regedit -p -r HKLM/Software/checkpoint/SIC` and reading the value of the CertPath parameter.

00380939 During SPLAT or Linux Endpoint Security installation, if you do not define a valid administrator, you will not be able to view events in the Endpoint Security reports. You must define a valid administrator during the install process.

00382778 When installing Endpoint security on Linux, if you cannot launch SmartPortal, use the following workaround:

1. Edit the `/etc/hosts` file and make sure the following entry exists:

   ```
   127.0.0.1 machine's real IP machinehostname
   ```

2. Connect to the machine with SmartConsole.

3. Edit the Integrity object.

4. Set the IP address, and choose install Database.

00382764 Sometimes, after switching from Standby to Active Server, you may need to restart the services.

**Client Installation, Upgrade, and Backward Compatibility**

00222314 The Custom Parameter RESETCONFIG to keep personal policy during upgrade is not supported. This affects the Flex users who have configured their client rules through the client UI. User settings are always deleted during upgrade and re-connection to the server. Passwords and upgrade keys are kept during upgrade.

00317079 Clients cannot download packages from an external source when they are restricted. If the client becomes restricted due to a client Enforcement rule, and the rule specifies an upgrade package on an external URL, the client may not be able to download the external package. This can occur even if the external URL is actually the same as an Endpoint Security Distribution Utility. A workaround is to upgrade using the Upgrade package from Endpoint Security Distribution Utility option rather than upgrading from an external URL.

00350782 When you install a client without VPN on an endpoint computer with R60 SecureClient installed, SecureClient will not function properly because of a conflict with SmartDefense. (This conflict does not occur when you install VPN clients, which replace SecureClient.)

**Workaround:** Install VPN client packages to replace SecureClient. (See the section on Migrating from Check Point SecureClient in the Endpoint Security Distribution Utility Administrator Guide.) Alternatively, disable SmartDefense in the client installation package. You can do this in the Client Packager by specifying the custom parameter INSTALL_SD=NO.
Resolved Limitations

The Custom Parameter REBOOTPROMPTWITHSILENT only affects installations when using an msi installer that was created from a Client Package using the msi option. The Custom Parameter does not affect an install that is run using a Client Package directly, including upgrades initiated via enforcement rules.

Before upgrading an existing GPO installation using manual upgrade or automatic update feature, you must verify the existing GPO configurations are removed from the client system.

Perform the following steps on the GPO server:
1. Select the installed package, right click, and choose All Tasks > Remove.
2. Select Allow users to continue to use the software, but prevent new installations.
   - This ensures the GPO settings are cleared on the client's registry but leaves the software on the system.
   - When the client receives the updated policy, the application settings are removed from the following GPO Application Management registry key:
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\AppMgmt
3. Proceed with manual or automatic upgrade.

When performing a GPO upgrade, the existing Check Point Endpoint Security client's disconnected policy must contain a firewall rule that allows outbound traffic to the GPO server's IP. If this is not configured, the upgrade process will not be able to remove the existing software correctly and the GPO upgrade will fail.

Integration

If you see an unexpected error when logging into Endpoint Security Distribution Utility with your SmartCenter administrator credentials, it may be because your SmartCenter license has expired or become invalid. If you are running Endpoint Security Distribution Utility together with SmartCenter (either on the same host or on separate hosts), and your SmartCenter license expires or becomes invalid, you are not able to log on to Endpoint Security Distribution Utility using your SmartCenter administrator credentials. This occurs whether you are trying to log on to Endpoint Security Distribution Utility directly or through SmartDashboard. Use the cplic command to check the status of your SmartCenter license, and if necessary, set a new SmartCenter license. (For information on cplic, see the Check Point Command Line Interface Guide.) Even if your SmartCenter license is invalid, however, you can log in to Endpoint Security Distribution Utility using your Endpoint Security Distribution Utility administrator credentials.

If you are setting up a distributed installation (in which Endpoint Security Distribution Utility and SmartCenter run on separate hosts), Endpoint Security Distribution Utility does not automatically synchronize with SmartCenter. To synchronize Endpoint Security Distribution Utility with SmartCenter, restart Endpoint Security Distribution Utility after you install and configure SmartCenter, install the database, and establish secure internal communication (SIC).

If you are setting up a distributed installation (one in which Endpoint Security Distribution Utility and SmartCenter run on separate hosts), changing the logging settings to store Endpoint Security Distribution Utility logs locally will result with an authentication error on every attempt to view logs from within Endpoint Security Distribution Utility. In this configuration, you can view the logs with SmartView Tracker or Smart Portal.
Resolved Limitations

00326849 After installing an Endpoint Security Distribution Utility on a Provider-1 MDS machine, perform the following steps to prevent a crash:

1. Stop the CMA that works with the Endpoint Security Distribution Utility.
2. Log out of the shell used to start the Endpoint Security Distribution Utility installation.
3. Log in again to the root account.
4. Start the CMA.

After upgrading a Provider-1 MDS server that includes an installation of Endpoint Security Distribution Utility that is associated with one of the CMAs, perform the same procedure.

Logging, Alerts, and Errors

00208493 Endpoint Security Distribution Utility 7.0 is now certified to support 20,000 concurrent endpoint users with default configuration. Higher performance figures are possible with customization for your environment. Contact Check Point Professional Services for information about configuration for more than 20,000 concurrent endpoint users.

00222872 After installing a distributed Endpoint Security server (with a remote Smart Center), configuring the SIC communication, and installing the database, you must restart the Endpoint Security server machine in order to complete the configuration.

00311753 Continuous looping of log uploads occurs if the minimum number of events is less than 2. In order to prevent continuous looping of log uploads, in the Client Configuration > Client Settings panel’s Log Upload Size area, set the minimum number of events to be equal to or greater than 2.

00313304 While Apache is running, it shows the following error: (730038)An operation was attempted on something that is not a socket.: winnt_accept: AcceptEx failed. Attempting to recover. Workaround: Place the directive Win32DisableAcceptEx on a separate line in the beginning of the httpd.conf configuration file (in install_dir\apache2\conf), and then restart Apache.

00318085 Logging at the Info level can produce a lot of data. For this reason, do not set Info level notifications to be sent to e-mail.

00374651 After upgrading an Endpoint Security server version 6.5.x to version 7.x, the Smart Portal IP and port will not be correctly configured.

To configure:

1. Log into the Endpoint Security server.
2. Go to System Configuration > Server Settings.
3. Click Edit.
4. Enter the correct Endpoint Server IP address and port for Smart Portal (default Smart Portal port is 4433. For example: 209.87.213.90:4433).
5. Click Save.

00374929 When installing Endpoint Security Distribution Utility in conjunction with other products from the wrapper on Linux and SPLAT, the Endpoint Security server is not configured properly until you run Smart Dashboard and install the database on the local machine.
00375433 Due to an issue in the SmartCenter import/export mechanism (existing in SmartCenter R65, and, possibly previous versions as well), when exporting and then importing a SmartCenter configuration in environments where the Endpoint Security server is managed by the SmartCenter, the communication between SmartCenter and the Endpoint Security server will cease functioning.

Workaround: Run the command `cpprod_util SetCertPath ($CPDIR)/conf/sic_cert.p12` using the value of `$CPDIR`. You can verify this (on Linux or SPLAT) by using `ckp_regedit -p -r HKLM/Software/checkpoint/SIC` and reading the value of the CertPath parameter.

00380939 During SPLAT or Linux Endpoint Security installation, if you do not define a valid administrator, you will not be able to view events in the Endpoint Security reports. You must define a valid administrator during the install process.

00382778 When installing Endpoint security on Linux, if you cannot launch SmartPortal, use the following workaround:

1. Edit the `/etc/hosts` file and make sure the following entry exists:

   ```
   127.0.0.1 machine's real IP machinehostname
   ```

2. Connect to the machine using SmartConsole.

3. Edit the Integrity object.

4. Set the IP address, and choose install Database.

00382764 Sometimes, after switching from Standby to Active Server, you may need to restart the services.

**Localization and Special Characters**

00313520 Classic Firewall Rules cannot contain certain symbols. You cannot use the ampersand symbol (`&`), quotation marks, or the less than symbol (`<`) in the names of Classic Firewall Rules.

00314811 Using Client Rules to update clients of different locales (languages) is not supported. The rules are applied regardless of the client locales, which results in all clients being updated to the same language. Workaround: Assign a different policy with a different Client Rule to each client with a different locale. You can move all users back to a shared policy after the upgrade has completed.

00315851 Localized characters are not supported in the Install Key. You cannot use non-English characters in the Install Key in the Client Packager page. Workaround: Use only ascii characters for the Install Key.

00320198 In search fields in the Endpoint Security Distribution Utility administration console, Endpoint Security Distribution Utility interprets the characters `"%"` and `"_"` as search wildcards, NOT as literal characters for which to search.

**Gateways and Third Party Product Integrations**

00307263 In order for the Endpoint Security client to detect McAfee Virus Scan Enterprise Virus definition, you must use the full McAfee product version number when referencing it for the Endpoint Security client. This is because the McAfee product's user interface displays only a portion of the product version number.
Resolved Limitations

00309474 SecureClient is not compatible with PC-Cillin 2005. If you have SecureClient installed, you will not be able to also install PC-Cillin 2005.

00316842 A personal policy is not able to block Microsoft Remote Desktop. You cannot block Microsoft Remote Desktop using application rules.

00322997 If you are using EAP and the Network Interface Card is disabled, it will remain disabled even after reboot.

00327385 If a client is out of compliance with an Enforcement Rule that is configured to Warn or Observe, the VPN Security Configuration (or SCV status) is displayed as Verified. It is displayed as Not Verified only if the Enforcement Rule is configured to Restrict the client.

00369461 Endpoint Security clients don’t recognize full version numbers for Sophos antivirus products. Endpoint Security clients only recognize version numbers up to two places after the first decimal point (x.xx).

Miscellaneous

00209761 Scheduled Antispyware scan times can be incorrect when the Endpoint Security server and the Endpoint Security client are located in different time zones. This is because the scan time always occurs at the specified time in the server's time zone instead of the client's time zone.

00313856 Internet Explorer (6.x) limits to 3000 the number of groups you can import into an NT Domain, LDAP, or RADIUS catalog on Endpoint Security Distribution Utility. To import more than 3000 groups, use another of the supported browsers. Mozilla Firefox is the only compatible browser that accommodates imports of more than 10,000 groups. For very large imports, the import page may take up to ten minutes to display all imported groups. When importing groups with a browser other than Internet Explorer, users may get a warning asking whether to abort the long-running javascript routine. Users should close the dialog box or choose to continue running javascript. For Firefox, you can suppress this message by typing about:config in the address bar, finding the entry for dom.max_script_run_time, and setting the number to 60 (on new computers) or 120 (on older computers).

00315338 The Flex client must be rebooted to register changes to Return to Default buttons. When you change the setting of Hide Return to Default buttons in Flex (in the Advanced Settings section of a policy's Client Settings tab), the end user must reboot the Flex client for the change to take effect.

00316817 Enterprise policies cannot override keyboard and mouse settings. If a policy allows a program and to enforce the enterprise policy only, and the user has set permissions in the personal policy to block the program, the program is able to access the Zones as defined in the enterprise policy, but is not able to perform keyboard and mouse activity. Workaround: Users must set the program to allow the keyboard and mouse activity in the personal policy.

00352091 Endpoint users in the Test Group do not receive automatic updates if Antivirus or Antispyware staging is not configured. Do not place users in the Test Group unless you also configure staging.

00367804 It is possible to block Antivirus and Antispyware updates with firewall rules. Be sure to configure your firewall rules to allow this traffic.
00368783 Updates will sometimes fail after initial installation due to file permissions issues. This update failure is not common and subsequent updates are generally successful.

00368936 The traceroute protocol cannot be used to block trace route outbound. In order to prevent traceroute from working, block the traceroute program with an Application Rule. Alternatively, you could block the inbound ICMP timeout packet, but this may cause issues.

00374371 When a client is in disconnected mode and has an active disconnected policy it will not ask the server for permissions of programs. Therefore all programs not explicitly overridden in the policy will be treated as "unknown" and will be given permissions according to the "unknown programs" group filter.

00378440 There are no implied rules to allow remediation or Antivirus or Antispyware updates. Do not configure firewall rules that block this traffic.

00379172 Logitec QuickCam software version 10.5 is incompatible with the Check Point Endpoint Security client. This causes crashes of many programs when they attempt to start. You must upgrade to version 11.5 of the Logitec QuickCam software.

00382005 Endpoint Security will not install on endpoint computer that have any active firewalls other than the Microsoft built-in firewall.

VPN

00209078 Entrust configuration is not supported in Endpoint Security Distribution Utility VPN packages. When you need Entrust configuration, install the Endpoint Security client and SecureClient separately.

00209079 You cannot configure script execution.

If you need script execution for SCV enforcement, you must install an Endpoint Security client and SecureClient separately.

00320920 When using "Route all traffic through gateway" in conjunction with Office Mode in Endpoint Security with VPN, with SCV enforcement on Endpoint Security, the client sometimes sends packets from the real IP rather than the Office Mode IP. Microsoft Windows Dead Gateway Detection causes this behavior as it handles the default route. To avoid this change the EnableDeadGWDetect registry key. More information can be found in the SecureKnowledge SK39013 article.

To disable the Dead Gateway Detection mechanism on NG AIR R54 and R55, modify the registry as follows:

**Note:** Always back up the registry before making any modification.

1. Select Start > Run.
2. From the Run dialog box, under the Open field, execute the regedit command.
3. Locate the HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters section.
4. Add the following DWORD with the value "0" EnableDeadGWDetect.
5. Save and exit.
6. Reboot.
Some buttons on VPN dialogs are not the default button even though they are highlighted as such. This will cause keyboard shortcuts to select different controls than highlighted.

For Firewall-1, the Implied/Hard-Coded rules that are applied before all policy rules don't include the new Endpoint Security ports and protocols. You must configure firewall rules to allow Endpoint Security traffic. Use the following steps:

1. Make a copy of the implied_rules.def file on SmartCenter and save it.
2. Under INTEGRITY_HEARTBEAT, change port 6054 to 80.
3. Under accept_integrity_server_ports, change port 80 to 2100.

Example:

```c
#define INTEGRITY_HEARTBEAT (udp, dport = 80)
#else ENABLE_INTEGRITY_SERVER_TRAFFIC
#define accept_integrity_server_ports(targets)
  all@targets accept
  (tcp, dport = 5054,
   src in integrity_list, dst in firewalled_list,
   start_rule_code(0),
   IMPLIED_LOG
  ) or ( (tcp, (dport = 443 or dport = 2100)) or
    INTEGRITY_HEARTBEAT),
    ( (inbound, ifaddr in internal_interface_list)
      or src in gui_clients_list ),
    dst in integrity_list,
    start_rule_code(0),
    IMPLIED_LOG,
    IMPLIED_RECORD_CONN(MAKE_RULENUM(0,0x08)),
    IMPLIED_LOG,
    (call KFUNC_SET_BITS<SAM_DONT_CLOSE_ID, 1> or 
     1)
  );
```

4. Save the file.

Note that editing the implied_rules.def file must be done carefully and only for important workarounds.

The local subnets feature of Hotspot Registration is not enforced. Setting Hotspot.local.subnets.only to 'true' has no effect.

When using the Cingular WWAN Connection Manager, it may conflict with Endpoint Security VPN client. When switching to the WWAN adapter, the Endpoint Security VPN client may switch to CLI mode.
**Version 7.0 HFA 01 Resolved Issues**

00374371 00223543 Unconnected endpoints did not get program group permissions.

Resolution: You now have the option to include program group permissions in a policy, so that these permissions will be used when the endpoint computer is unconnected with the Endpoint Security server. Enterprises are limited to five such Filter Groups because of the performance issues associated with including large numbers of program permissions in policies.

00311759 The method for enabling SYSLOG and SNMP traps in Linux was not documented.

Resolution: The method for enabling SYSLOG and SNMP traps in Linux is now documented in the Administrator Guide.

00197450 Smart Defense policy files (enabled policy and disabled policy) protection values lead to false positives.

Resolution: Fixed an issue in Smart Defense that could cause false positives.

00223348 Installation fails due to missing a root certificate.

Resolution: Root certificate is correctly configured during client installation.

00223367 No option to disable wireless on LAN.

Resolution: The Disable Wireless on LAN feature is now available. Activate it in the policy Client Settings tab.

00223544 7.0 Endpoint Security servers do not support 7.1 clients although they are in fact 6.5 clients with a nonsequential version number.

Resolution: Connections from Integrity 7.1 vista clients is now supported. However, these clients cannot be packaged with Check Point Endpoint Security 7.0 or greater.

00353336 Problem: Scan window doesn't have the option to hide.

Resolution: The scan progress window can now be properly minimized.

00377341 Problem: VSMON memory leak.

Resolution: Memory leak fixed.

00378028 SOD related to third-party hooking.

Resolution: BSOD related to third-party hooking fixed.

00381633 Reporting problems for Full Disk Encryption and Media Encryption.

Resolution: Better reporting added to the Endpoint Detail report.

00382685 Register to hotspot' option in Endpoint Security client is not deselected after connecting to VPN

Resolution: Register to Hotspot tray menu item is now deselected after connecting to VPN.
Resolved Limitations

00382700 Pop-up that hotspot registration is enabled doesn't appear
   Resolution: User experience for Register to Hotspot feature improved.

00408642 The "Review compliance alert" option isn't working.
   Resolution: Compliance Review feature functionality improved.

00411382 Auto Local Logon allows credential theft
   Resolution: Fixed a security issue related to Auto Local Logon.

00411387 Fingerprint accepted without user's confirmation
   Resolution: Fixed a security issue related to Fingerprint acceptance without user confirmation.

00413635 Changing the datastore ‘Number of Backups to keep’ setting causes a java exception
   Resolution: The number of datastore backup to keep can now be changed without causing an exception.

00413700 When creating Enforcement Rules, Win2003 OS and Vista do not appear in the drop down list.
   Resolution: You can now specify Enforcement Rules for Windows 2003 Server and Vista. Currently, only the Integrity 7.1 client supports Vista.

00413861 In the Windows XP Hebrew edition all yes/no ok/cancel buttons in dialog boxes are gibberish.
   Resolution: VPN confirmation dialogs have correct button text for client installations on foreign OS.

00417381 Blue screen is received while trying to connect with Secure Client.
   Resolution: Fixed BSOD related to connecting to the VPN.
Documentation Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.co