This package contains: CPSECPEP010S **Version 2.0** July 08 / 2008

1. PEP Number: CPSECPEP010S Version 2.0

Summary:

a). List of CRs resolved in this PEP, section 3.1
b). List of hotfixes installed by this PEP, section 3.2
c). List of registry changes, section 3.3
d). List of services being disabled, section 3.4
e). Disk space requirements. section 4e.
f). Opsware related info, section 9
g). Hotfix checker, section 10

2. Problem Description

This package contains Microsoft hotfixes to be installed on a CallPilot 3.0, 4.0 or 5.0 server. Certain additional OS hardening and enhancement are also made to improve security.

The PEP contains all applicable hotfixes from the time Windows Server 2003 SP1 was originally released up to and including Feb 12th, 2008 (Up to MS08-013 but excluding IE7 and SP2). It can be installed on SP1 and SP2 systems, and will coexist with CPSECPEPSP2S if present in DMI and Windows Add/Remove programs list.

Installation can take up to 50 minutes depending on your platform and CallPilot release. Less time is needed if anti-virus software is temporarily disabled during installation. This PEP may be installed remotely using pcAnywhere or Remote Desktop.

NOTE: Do not apply this security PEP CPSECPEP010S to CallPilot 4 servers which have already been JITC hardened since the PEP may weaken some of the security hardening needed for JITC compliance.

KNOWN ISSUE: After installing this PEP on a CallPilot server without CPSECPEPSP2S, backup to a network drive will not work. When you try to map the network drive, you will get an error "The account is not authorized to log in from this station". There are two solutions for this problem:
a) install CPSECPEPSP2 to upgrade to Windows Server 2003 Service Pack 2 (recommended)
b) Use Administrator Tools > Local Security Policy > Security Options. Change the "Microsoft Network Client Digitally sign communications (always)" setting to "Disabled" and reboot the server

KNOWN ISSUE: After installing this PEP, the High Availability Configuration Wizard will get an error "Unable to connect to the registry on server". The workaround for this is to temporarily manually start the Remote Registry service. Use the Services applet to set the service to manual, then start it. (This problem Q01846574 will be addressed by a change to the wizard in CP5 SU04).

3.1 List of CRs that are fixed by this PEP

Q01367189 - Excessive TCP Keep-Alive LAN traffic with Desktop Messaging
Q01449531 - DMI view update sets CPservices to disabled after installing PEP CP202SEC004S
Q01617017 - MSI-Format support for CallPilot
Q01638452 - CP40404SU04S failed to install on a 703t with CallPilot 4.0 GA
Q01637569 - Receiving numerous event 59 and 32 in system log
Q01781913 - PEP CPSECPEP009S crashes CallPilot

Q01783689 - Need Windows Administrator account to launch CallPilot Manager Homepage
Q01806764 PEP CPSECPEP010S makes many main functions of CallPilot work incorrectly
Q01807104 CPSECPEP010S – Some securities are not added as expectation
Q01807140 Some enhancement securities are not configured properly
Q01807505 Users can configure proxy setting in IE
Q01807989 Service “Help And Support (helpsvc)” is not configured as document mentioned
Q01819385 Cannot login to Support Tools on CP sever joined to Domain
Q01819279 Some registries are not added as expected

3.2 list of hotfixes to patch the following Microsoft Bulletins

MS05-026 Jun 14/2005 Vulnerability in HTML Help Could Allow Remote Code Execution (896358)
MS05-033 Jun 14/2005 Vulnerability in Telnet Client Could Allow Information Disclosure (896428)
MS05-036 Jul 12/2005 Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)
MS05-039 Aug 8/2005 Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
MS05-040 Aug 8/2005 Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)
MS05-041 Aug 8/2005 Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (899591)
MS05-042 Aug 8/2005 Vulnerabilities in Kerberos Could Allow Denial of Service, Information Disclosure, and Spoofing (899587)
MS05-045 Oct 11/2005 Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)
MS05-046 Oct 11/2005 Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)
MS05-048 Oct 11/2005 Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (901017)
MS05-049 Oct 11/2005 Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)
MS05-051 Oct 11/2005 Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)
MS06-002 Jan 10/2006 Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (908519)
MS06-006 Feb 14/2006 Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution (911564)
MS06-008 Feb 14/2006 Vulnerability in Web Client Service Could Allow Remote Code Execution (911927)
MS06-014 Apr 11/2006 Vulnerability in the Microsoft Data Access Components (MDAC) Function Could Allow Code Execution (911562)
MS06-015 Apr 11/2006 Vulnerability in Windows Explorer Could Allow Remote Code Execution (908531)
Dec 12/2005 Update for Windows Server 2003 (KB910437)
MS06-022 Jul 26/2006 Vulnerability in ART image rendering could allow remote code execution (918439)
MS06-024 Jul 26/2006 Vulnerability in Windows Media Player could allow remote code execution (917734)
MS06-030 Jul 26/2006 Vulnerability in Server Message Block could allow elevation of privilege (914389)
MS06-025 Aug 8/2006 Vulnerability in Routing and Remote Access could allow remote code execution (911280)
MS06-036 Aug 30/2006 A vulnerability in the DHCP Client Service could allow remote code execution (914388)
MS06-041 Aug 30/2006 Vulnerability in DNS resolution could allow remote code execution (920683)

MS06-043 Aug 30/2006 Vulnerability in Microsoft Windows could allow remote code execution (920214)
MS06-046 Aug 30/2006 Vulnerability in HTML Help could allow remote code execution (922616)
MS06-050 Aug 30/2006 Vulnerabilities in Microsoft Windows Hyperlink Object Library could allow remote code execution (920670)
MS06-040 Sep 12/2006 Vulnerability in Server service could allow remote code execution (921883)
MS06-053 Sep 12/2006 Vulnerability in Indexing Service could allow cross-site scripting (920685)
Sep 09/2006 Update for Windows Server 2003 (KB922582)
MS06-057 Oct 10/2006 Vulnerability in Windows Explorer Could Allow Remote Execution (923191)
MS06-063 Oct 10/2006 Vulnerability in Server Service Could Allow Denial of Service and Remote Code Execution (923414)
MS06-064 Oct 10/2006 Vulnerabilities in TCP/IP IPv6 Could Allow Denial of Service (922819)
MS06-065 Oct 10/2006 Vulnerability in Windows Object Packager Could Allow Remote Execution (924496)
MS06-066 Nov 14/2006 Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution (923980)
MS06-068 Nov 14/2006 Vulnerability in Microsoft Agent Could Allow Remote Code Execution (920213)
MS06-074 Dec 12/2006 Vulnerability in SNMP Could Allow Remote Code Execution (926247)
MS06-075 Dec 12/2006 Vulnerability in Windows Could Allow Elevation of Privilege (926255)
MS06-078 Dec 12/2006 Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689 & 925398)
MS07-004 Jan 09/2007 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)
MS07-006 Feb 13/2007 Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)
MS07-008 Feb 13/2007 Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)
MS07-011 Feb 13/2007 Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)
MS07-012 Feb 13/2007 Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)
MS07-013 Feb 13/2007 Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)
MS07-017 Apr 03/2007 Vulnerabilities in GDI Could Allow Remote Code Execution (925902)
MS07-020 Apr 10/2007 Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)
MS07-021 Apr 10/2007 Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)
MS07-022 Apr 10/2007 Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)
MS07-031 Jun 12/2007 Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)
MS07-033 Jun 12/2007 Cumulative Security Update for Internet Explorer (933566)
MS07-034 Jun 12/2007 Cumulative Security Update for Outlook Express and Windows Mail (929123)
MS07-035 Jun 12/2007 Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)
MS07-039 Jul 10/2007 Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)
MS07-040 Jul 10/2007 Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)

MS07-042 Aug 14/2007 Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)
MS07-046 Aug 14/2007 Vulnerability in GDI Could Allow Remote Code Execution (938829)
MS07-047 Aug 14/2007 Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782)
MS07-050 Aug 14/2007 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)
MS07-056 Oct 9/2007 Security Update for Outlook Express and Windows Mail (941202)
MS07-058 Oct 9/2007 Vulnerability in RPC Could Allow Denial of Service (933729))
MS07-061 Nov 13/2007 Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460)
MS07-028 Vulnerability in CAPICOM Could Allow Remote Code Execution (931906)
MS07-064 Dec 11/2007 Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)
MS07-067 Dec 11/2007 Vulnerability in Macrovision Driver Could Allow Elevation of Privilege (944653)
MS07-068 Dec 11/2007 Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275)
MS08-001 Jan 08/2008 Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)
MS08-002 Jan 08/2008 Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)
MS08-005 Feb 12/2008 Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)
MS08-006 Feb 12/2008 Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830)
MS08-007 Feb 12/2008 Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)
MS08-008 Feb 12/2008 Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)
MS08-010 Feb 12/2008 Cumulative Security Update for Internet Explorer (944533)

KB890830 Windows Malicious Software Removal Tool
KB910437 Windows Automatic Update, access violation error
KB911897 Files corrupted on Windows Server 2003-based computer when you try to use the local UNC path to copy the files
KB922582 Error message when you try to update a Microsoft Windows-based computer: “0x80070002”

KB927891 Update for Windows Installer (MSI)
KB942840 Update for Windows Server 2003 (KB942840)
Adobe Reader Security bulletin - Update available for vulnerability in versions 8.1 and earlier of Adobe Reader and Acrobat
http://www.adobe.com/support/security/bulletins/apsb07-18.html

Update for Windows Server 2003 (KB942840)
Visual Basic 6.0 Service Pack 6 oleaut32.DLL Security Update (KB946235)

3.3 Changing Registry settings for improved security

Set threshold for Windows disk full warning to 2 percent
Enable signatures on SMB
Disable updating of Last Access Time by NTFS
Set Event Log sizes, retention policy and guest access
Remote Access Settings- disallow saving password, enable logging, and answer after 5 rings

Remote Access Settings- Authentication Retries 6, Time 2 min, auto disconnect 2 min, KeepConn 5 min

Set KeepAliveTime to 300,000 ms according to MS recommendation.

Disable AutoRun on all drives

Set ScreenSaver Grace Period to 0

Make proxy settings per-machine (Disallow per-user proxy settings)

Prevent Internet Explorer from automatically downloading new software to update/upgrade itself

Ensure that software update shell notifications are enabled

Tighten the handling of temporary directories used by Terminal Services (Remote Desktop) sessions

Remove Installer Policies Key to ensure that no elevated privileges have been given to the Installer

Although the Posix subsystem was already disabled, remove an additional registry key associated with Posix

Remove the default password for use if autologin was configured from the registry

Enable SaveDLLSearchMode to make it harder for an attacker to introduce malicious software in the form of a DLL

Disable Remote Desktop Sharing (as used by Microsoft conferencing products)

Use only machine settings (not per user) for IE Security Zone Settings

Tighten restrictions on Remote Desktop Connections

Prevent the installation of Microsoft Messenger Client

Disable PCHealth Error Reporting to Microsoft

Prohibit the use of Internet Connection Sharing

Block the installation of Kernel Mode Printer drivers (most printer drivers are not kernel mode today)

Prevent Windows Media Player from automatically downloading and installing new codecs and updates

Disable Messenger Client and Messenger Service software

Registry flag changes to protect against a security issue with the Macromedia Flash Player

Workaround for MS06-041: Modifying the Autodial DLL within the Windows registry will prevent an application, specially crafted
website or e-mail message from calling the affected API and exploiting the vulnerability.

Workaround for MS06-042: Disable caching of Web content in Internet Explorer

Internet Zone- Control Access to data sources across domains based on the site being browsed

Local Zone- Control Access to data sources across domains

Trusted Sites Zone- Control Access to data sources across domains

Restricted Sites Zone- Ensure Active Scripting has level of protection based on site being accessed

Trusted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting (prompt)

Local Zone- Prevent execution of ActiveX controls not marked safe for scripting (prompt)

Restricted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting

Internet Zone- Prevent execution of ActiveX controls not marked safe for scripting (prompt)

Restricted Sites Zone- Ensure Allow META REFRESH has level of protection based on the site being browsed

Internet Zone- Ensure paste operations via script have level of protection based on site being accessed

Local Zone- Ensure paste operations via script have level of protection based on site being accessed

Trusted Sites Zone- Ensure paste operations via script have level of protection based on site being accessed

Restricted Sites Zone- Ensure paste operations via script have level of protection based on site being accessed
Internet Zone- Ensure Display Mixed Content has level of protection based on the site being browsed
Restricted Sites Zone- Ensure Display Mixed Content has level of protection based on the site being browsed
Restricted Sites Zone- Ensure client certificates are not presented to web sites without the user's acknowledgement
Internet Zone- Ensure client certificates are not presented to web sites without the user's acknowledgement
Local Zone- Ensure client certificates are not presented to web sites without the user's acknowledgement
Trusted Sites Zone- Ensure client certificates are not presented to web sites without the user's acknowledgement
Internet Zone- Ensure Signed Active X controls cannot be downloaded
Local Zone- Ensure Signed Active X controls cannot be downloaded without prompt
Restricted Sites Zone- Ensure Signed Active X controls cannot be downloaded
Trusted Sites Zone- Ensure Signed Active X controls cannot be downloaded without prompt
Internet Zone- Ensure unsigned Active X controls cannot be downloaded
Restricted Sites Zone- Ensure unsigned Active X controls cannot be downloaded
Local Zone- Ensure unsigned Active X controls cannot be downloaded
Trusted Sites Zone- Ensure unsigned Active X controls cannot be downloaded
Restricted Sites Zone- Ensure Drag and Drop (and copy/paste) of files has level of protection based on the site being accessed
Internet Zone- Ensure Drag and Drop (and copy/paste) of files has level of protection based on the site being accessed
Ensure IE Error Reporting is disabled since it could send sensitive info to vendor
Restricted Sites Zone- Ensure file download is disabled
Internet Zone- prevent download of fonts without a prompt
Restricted Sites Zone- prevent download of fonts
Ensure user is warned when changing zones
Ensure user is warned when IE form data is redirected to another site
Local Zone- set to a custom level so other required settings can take effect
Restricted Sites Zone- set to a custom level so other required settings can take effect
Trusted Sites Zone- Ensure Trusted Sites zone is set to custom level
Ensure IE checks signatures on downloaded programs
Ensure IE warns of invalid certificates
Local Zone- Prevent execution of ActiveX controls not marked safe for scripting
Trusted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting (set to prompt)
Internet Zone- Prevent execution of ActiveX controls not marked safe for scripting (set to prompt)
Restricted Sites Zone- Prevent execution of ActiveX controls not marked safe for scripting (set to prompt)
Internet Zone- Prevent installation of desktop items
Local Zone- Prevent installation of desktop items without a prompt
Restricted Sites Zone- Prevent installation of desktop items
Trusted Sites Zone- Prevent installation of desktop items without a prompt
Local Zone- Set Java Permissions appropriate for Zone (prompt)
Internet Zone- Set Java Permissions appropriate for Zone
Trusted Sites Zone- Set Java Permissions appropriate for Zone
Restricted Sites Zone- Set Java Permissions appropriate for Zone
Local Zone- Control Launching Programs and files in IFRAME
Internet Zone- Control Launching Programs and files in IFRAME
Trusted Sites Zone- Control Launching Programs and files in IFRAME

Restricted Sites Zone- Control Launching Programs and files in IFRAME
Internet Zone- Control Frames trying to navigate across different domains
Restricted Sites Zone- Control Frames trying to navigate across different domains
Restricted Sites Zone- Control the running of ActiveX controls and plug-ins
Internet Zone- Control the scripting of Java applets (prompt)
Restricted Sites Zone- Control the scripting of Java applets
Internet Zone- Control Software Channel permissions
Local Zone- Control Software Channel permissions
Restricted Sites Zone- Control Software Channel permissions
Trusted Sites Zone- Control Software Channel permissions
Restricted Sites Zone- Control Submission of non-encrypted form data
Internet Zone- Control Submission of non-encrypted form data (prompt)
Restricted Sites Zone- User Authentication - Logon (control how credentials are passed to web sites)
Internet Zone- User Authentication - Logon (control how credentials are passed to web sites)
Local Zone- User Authentication - Logon (control how credentials are passed to web sites)
Trusted Sites Zone- User Authentication - Logon (control how credentials are passed to web sites)
Internet Zone- Control user data persistence
Restricted Zone- Control user data persistence

Enable Cipher setting for Triple DES 168/168 for all protocols
Enable Cipher setting for RC2 128/128 for all protocols
Enable Cipher setting for RC4 128/128 for all protocols
Enable Cipher setting for Skipjack for all protocols
Disable Cipher setting for NULL for all protocols
Enable MD5 and SHA Hashes for all protocols
Ensure IE SSL/TLS parameter allows SSL and TLS to be used from the browser
Disable Internet Printing Protocol

Set DCOM Static Allocation of Endpoints for NMAOS to ncacn_ip_tcp,0,5000 (always use port 5000)

Remove RunAs values in registry
MS06-067 - Prevent the Microsoft DirectAnimation Path ActiveX control from running in Internet Explorer
MS07-011 - Enable Embedded Object Blocking in Wordpad
MS07-020 - (Microsoft animated help agent)
MS07-045 - Set "kill bit" for certain COM objects:
MS07-047 - Disassociate the WMZ and WMD file extensions & Disassociation of WMZ and WMD in Windows prevents previewing or opening WMZ
and WMD files in Windows Media Player.
Visa scan result
Remote Desktop/Terminal Services settings:
Override user settings: End a disconnected session: 1 hour
Active Session Limit: Never
Idle Session Limit: 2 hours
Encryption level should be set to high
Disable Windows Print mapping, LPT Port mapping, COM mapping, Audio mapping
MS07-056 - remove news protocol handler to avoid Outlook news reader vulnerabilities
Disable SSLv2 since it is less secure and clients should be using SSLv3
Disable weak encryption algorithms (RC2 40bit; DES 56 bit; RC4 40bit; RC4 56bit; RC4 64bit)

Disable attempts to instantiate Microsoft Forms 2.0 ImageActiveX Control in IE

Disable COM object instantiation in IE
Internet Zone- .NET disable running components signed with Authenticode
Internet Zone- .NET disable running components not signed with Authenticode

3.4 Following services are set to disabled in order to reduce the attack surface

Application Layer Gateway Service (ALG)
Alerter (Alerter)
Application Management (AppMgmt)
ClipBook (ClipSrv)
DHCP Client (DHCP)
Distributed File System (Dfs)
Distributed Link Tracking Client (TrkWks)
Distributed Link Tracking Server (TrkSrv)
Error Reporting Service (ERSvc)
File Replication (NtFrs)
Human Interface Device Access (HidServ)
IMAPI CD-Burning COM Service (ImapiService)
Indexing Service (CiSvc)
Intersite Messaging (IsmServ)
Kerberos Key Distribution Center (kdc)
License Logging (LicenseService)
Local Display Manager (saldm)
Messenger (Messenger)
Microsoft Software Shadow Copy Provider (swprv)
NetMeeting Remote Desktop Sharing (mnmsrvc)
Network DDE (NetDDE)
Network DDE DSDM (NetDDEdsdm)
Network Location Awareness (Nla)
Portable Media Serial Number Service (WmdmPmSN)
Print Spooler (Spooler)
Remote Access Auto Connection Manager (RasAuto)
Remote Desktop Help Session Manager (RDSessMgr)
Remote Registry (RemoteRegistry)
Resultant Set of Policy Provider (RSoPProv)
Secondary Logon (seclogon)
Shell Hardware Detection (ShellHWDetection)
Smart Card (SCardSvr)
SNMP Trap Service (SNMPTRAP)
Special Administration Console Helper (sacsvr)
Task Scheduler (Schedule)
Telnet (TlntSvr)
Terminal Services Session Directory (Tssdis)
Themes (Themes)
Uninterruptible Power Supply (UPS)
Upload Manager (uploadmgr)
Virtual Disk Service (vds)
Volume Shadow Copy (VSS)
WebClient (WebClient)
Windows Audio (AudioSrv)
Windows Firewall/Internet Connection Sharing (SharedAccess)
Windows Image Acquisition (stisvc)
WinHTTP Web Proxy Auto-Discovery Service (WinHttpAutoProxySvc)
Wireless Configuration (WZCSVC)

3.5 Following services are set to manual in order to reduce the attack surface

Help And Support (helpsvc)
Logical Disk Manager (dmserver)

4. Pre-installation notes

a). Make sure you are installing this PEP on a CallPilot 3.0, 4.0 or 5.0 server

This PEP replaces the following PEPs if applicable:

- CP300SEC002S
- CP303SEC003S
- CP303SEC004S
- CP303SEC005S
- CP404SEC003S
- CP404SEC004S
- CP404SEC005S
- CPSECPEP006S
- CPSECPEP007S
- CPSECPEP008S
- CPSECPEP009S

The replaced PEPs will be automatically removed from DMI Viewer when CPSECPEP010S is installed.

b). Ensure there is a recent backup available prior to installing this PEP (or split RAID).

c). Make sure the CallPilot server is fully booted before beginning PEP installation.
Stop any other applications running on the local console, including all support tools and the CallPilot PEP Maintenance Utility (DMI Viewer).

d). Disable any active anti-virus software active on the server prior to installing this PEP. (This makes the PEP install faster.) As a precaution, it's recommended the CLAN connection be disconnected prior to disabling the anti-virus software.

e). Ensure sufficient free disk space.
This PEP will need 580 MB on C: to start installation process, actual final disk space consumption is less than 300 MB. Ensure the system has sufficient disk-space available to install this PEP. If required, use the following steps as needed to increase free disk space:

-If you set the User Environment Variable TMP (Start -> Control Panel -> System -> Advanced -> Environment Variables) to D:\TEMP\TMP, this will cause the CPSECPEP010S installer to unpack its files onto the D: drive instead of to the default temp folder (C:\Documents And Settings\Administrator\Local Settings\Temp). These actions will reduce the space on C: drive needed during the CPSECPEP010S install to 450 MB.

-Verify there is no unauthorized 3rd party software loaded on the CallPilot Server

-If Anti-Virus is installed, verify it is installed per Anti-Virus Bulletin P-2007-0101-Global. In particular, ensure that AV software is installed on the D: drive

-Clean any large unnecessary files and/or folders off the desktop. Once you have finished cleaning up, empty the recycle bin.

-Excessive space may be consumed by other Users. To find large files that are private to other users, using Windows Explorer, select C:\Documents And Settings, then click Search. Do not fill in any file name pattern, and click the "Search" button. This will display all files and folders that exist under this folder. Sort by size. If there are any large files shown, decide if they are needed.

Delete them or move them to another partition. Do not delete or move small files or shortcuts. Once you have finished cleaning up, empty the Recycle Bin.

- Delete hotfix uninstall folders C:\Windows\$NTUninstallKBnnnnnn$ (where nnnnnn is the Microsoft Knowledge Base article number). Once you have finished cleaning up, empty the Recycle Bin.
  For example: C:\Windows\$NTUninstallKB913580$
  Note: Folder KB931836 must remain on the system. Do not delete this folder.

-If needed, remove any unnecessary files and folders in the c:\temp or d:\temp folders. If an error occurs while attempting to remove a particular file, ignore the error, continue to remove as many other files and folders as possible in the temp folder. Note: do not remove the c:\temp and d:\temp, and D:\TEMP\CPSECPEP010S folders themselves. Once you have finished cleaning up, empty the recycle bin.

-If there is not enough disk space available on C: drive, please install CPDSKPEP001S. It will recover about 850MB on C: drive.

-If needed, use Windows Disk Cleanup utility to compress old files to save disk space:
Click Start->Programs->Accessories->System Tools->Disk Cleanup
Highlight C: drive and click OK, Disk Cleanup will analyze C: to determine the amount of space that can be freed. Select [Compress Old Files] in the Description section of the window. [Compress Old Files] is the only item which should be selected. De-select any other items, even if they were selected by default. Click OK and Yes to begin the disk cleanup process.

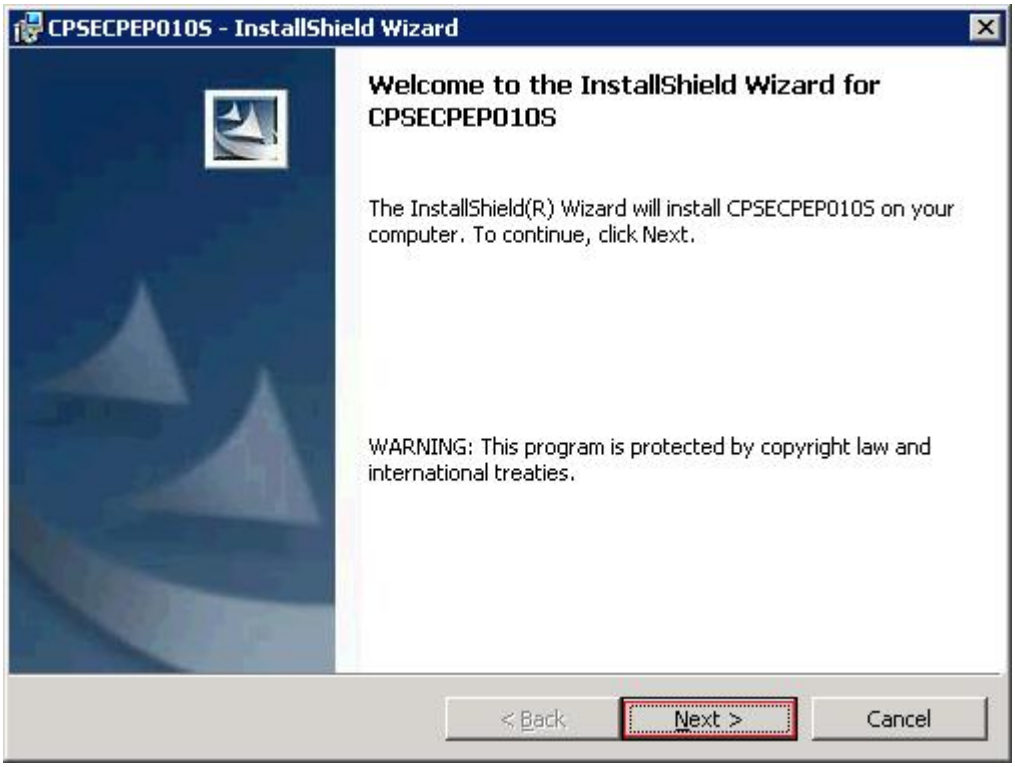
-If, after following the above steps, there is still not enough disk space available, CallPilot Manager can be removed prior to installing CPSECPEP010S and then re-installed. This uninstall/reinstall will temporarily free up 46MB on the C: drive and 76MB on the D: drive. Follow CallPilot Manager read-me file for un-install and re-install instructions.

-If the above actions do not free up enough disk space a case can be opened to investigate the space issue on a per site basis.

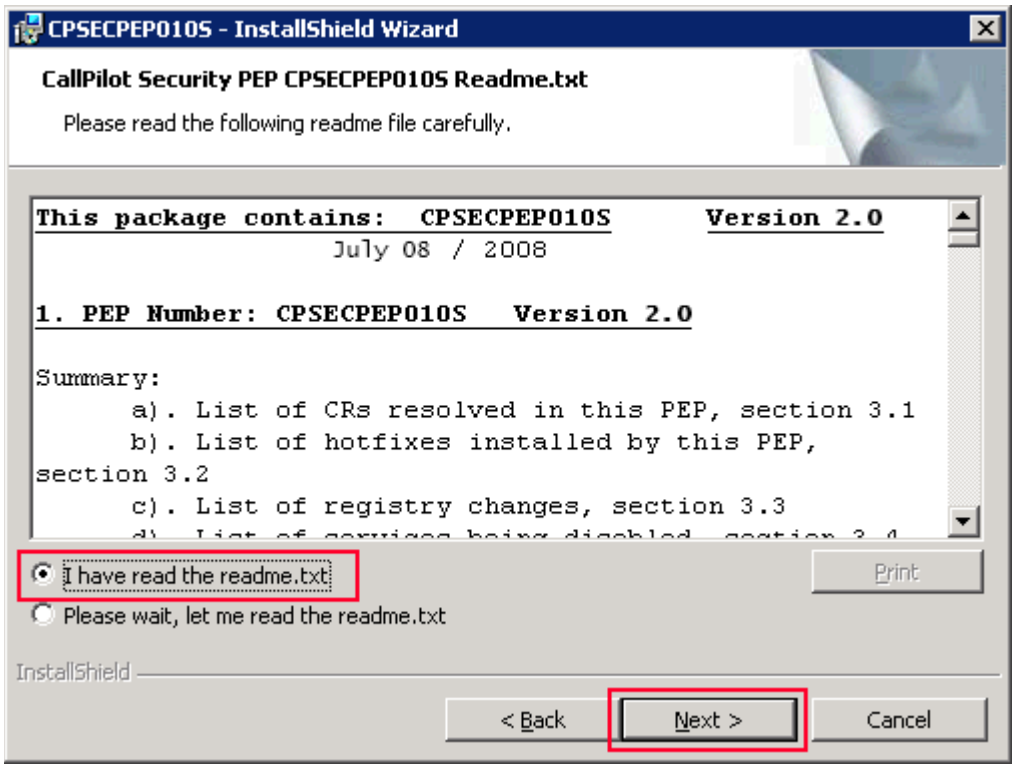
5. Installing the PEP

a). Begin installation by double-clicking on CPSECPEP010S.msi

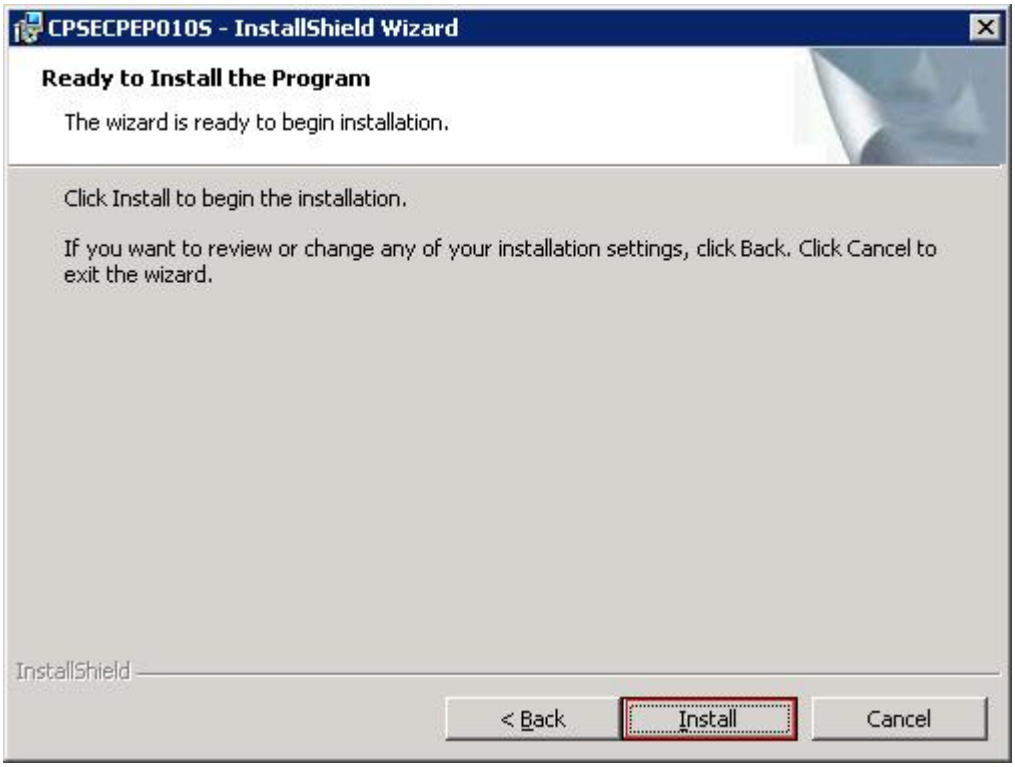
NOTE: If you run the MSI from a network location (e.g. a shared network drive), you will get an “Open File – Security Warning” window asking that “Are you sure you want to run this software?” just click on the Run button to run it.



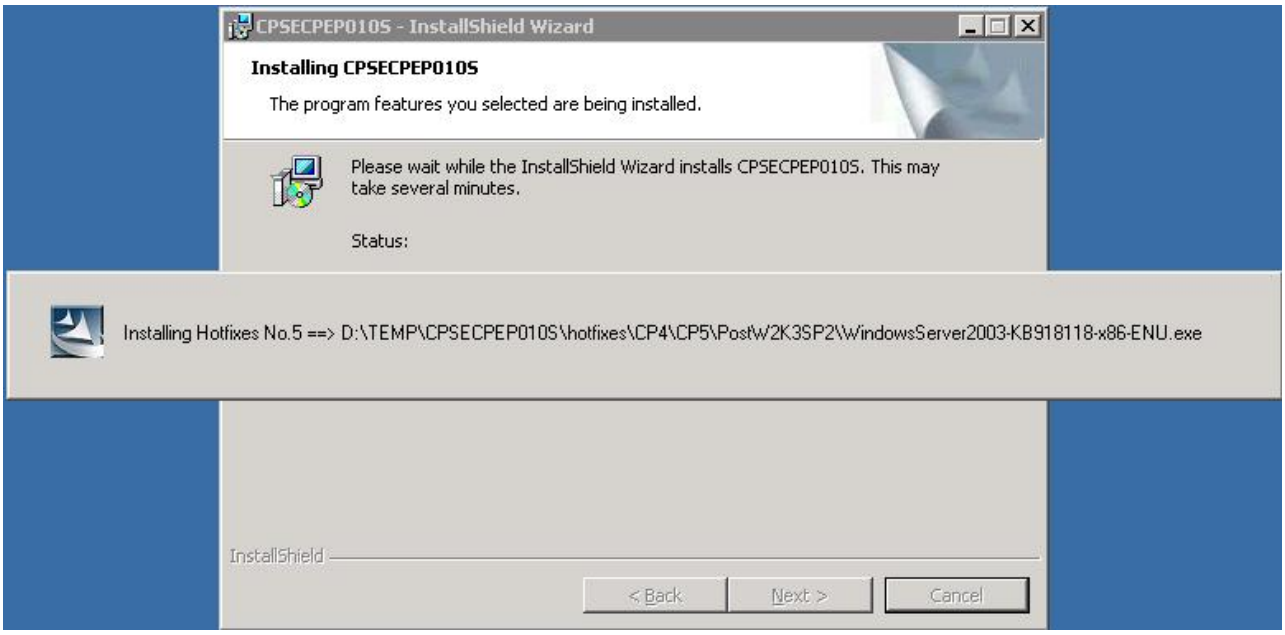
b). Click on Next button on window “Welcome to the InstallShield Wizard for CPSECPEP010S” and continue on to the Readme window.



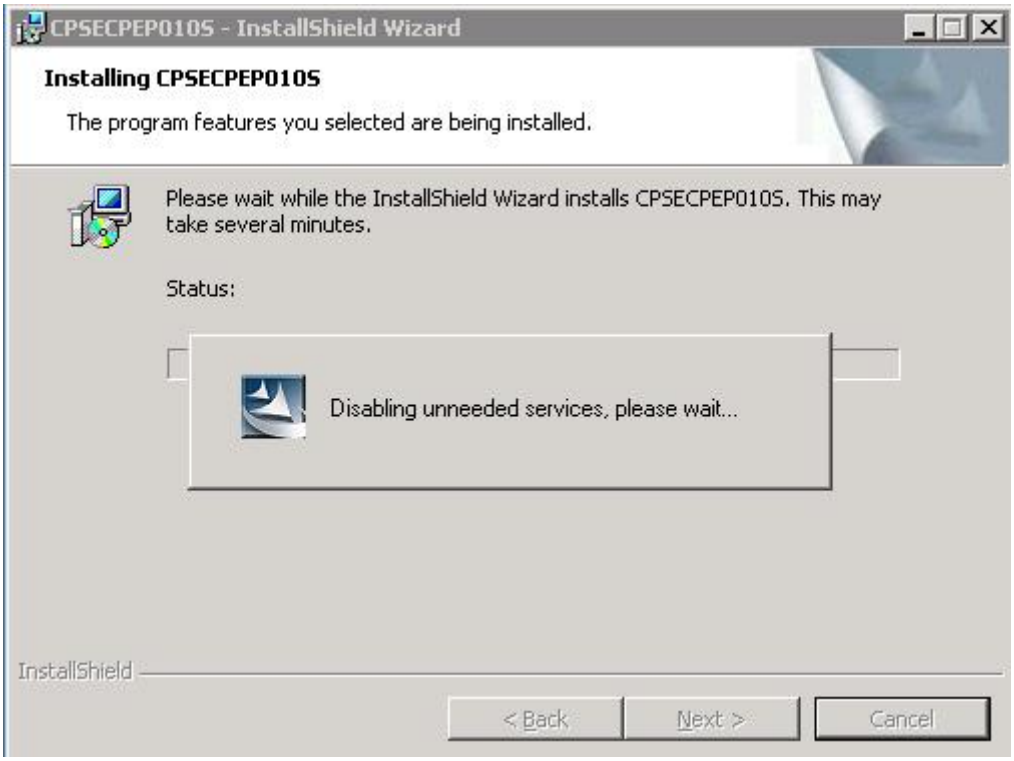
After reading through the readme, select Radio Button “I have read the readme.txt” and click on Next button.



On next window “Ready to install the Program”, click on Install button to install.

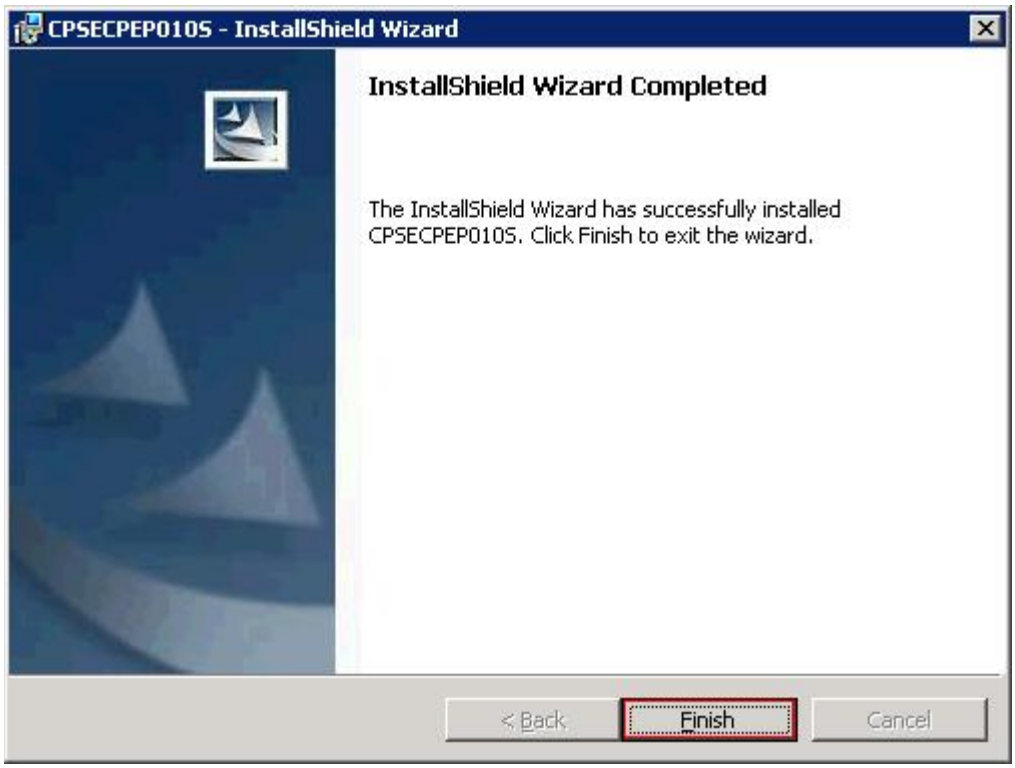


Note: Some cases, the main installation window “Installing CPSECPEP010S” will show up in front of the message box “Installing Hotfixes…”, that is a glitch of InstallShield, you may click on the message box and bring it to the front, either way will NOT affect the PEP install process.



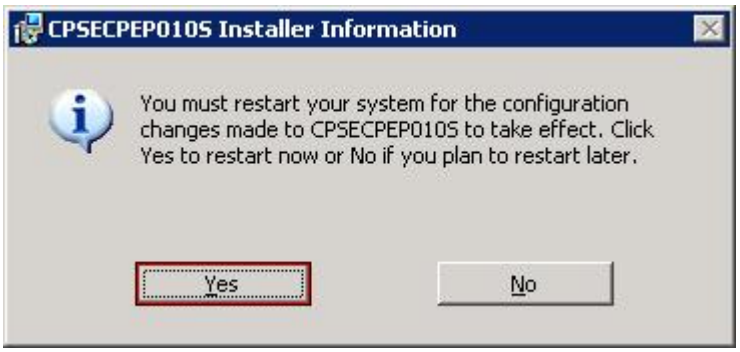
Note: Total time required will be about 50 minutes depending on your platform and CallPilot release, plus the time to reboot into service.

Note: This PEP automatically installs a number of Microsoft hot fixes. Do not close any windows or the PEP might not install successfully.



c). When the PEP installation is complete, a window will be displayed with the title "CallPilot OS Security PEP Installation Completed". Click on the Finish

button to exit the wizard, and then you will be prompted for option Yes to restart the server now and No to restart at a later time. You need a reboot to make the configuration changes to take effect.



NOTE: Although we don't recommend that you apply this PEP during busy hours, this PEP can be applied to a live server and the reboot can be deferred to a later time.

Note: Do not reboot the system until the PEP installation is finished, otherwise the PEP may not be properly registered on the server.

d). If anti-virus software was disabled, check to ensure it is now enabled. Note that it must be properly configured to scan "incoming" files only. See the bulletin P-2007-0101 on configuring anti-virus software for CallPilot.

6. Installation Log

File "SecPEP.log" in the root folder of the system drive will contain a log of the actions performed during PEP installation. In addition, a note will be added to the file "os_ver.txt", also in the root folder of the system drive.

7. PEP Uninstall

Due to the nature of the Microsoft hotfixes contained within this PEP, it cannot be uninstalled. Once applied, if removed from DMIViewer, only the references to PEP CPSECPEP010S in both DMIViewer and Windows Add/Remove Programs will be removed. Installation folder CPSECPEP010S under D:\TEMP will also be removed.

8. PEP Reinstallation

If required, this PEP may be installed again without any problem. Rerunning the PEP will reapply hotfixes and other configuration changes. If the PEP is not already in the PEP Utility (DMI Viewer), the PEP entry will be added when the PEP is reinstalled. If the PEP is already listed in the CallPilot PEP Utility (DMIViewer), it will not be added again to this utility.

9. Special installation instructions for Opsware:

No special instructions for installing this PEP via Opsware.

10. Supplemental Information - Verifying Hotfixes

To run the hot fix checker:
Double-click D:\TEMP\CPSECPEP010S\HotFixes\Checker\CheckHotFixes.bat

NOTE: The result (CheckResult.txt) will be opened in Notepad after the batch file execution; the result file contains two sections:

- Installed updates: list of all installed hotfixes.
- Missing Updates: list of missing hotfixes.