This package contains: **CPSECPEP016S** Version 1.0.0 Date: August 16 / 2013

1. PEP Number: CPSECPEP016S Version 1.0.0

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, 5.0 or 5.1 server. Certain additional OS hardening and enhancement are also made to improve security.

The PEP contains all post-SP2 applicable hotfixes up to and including August 13, 2013 (Up to MS13-066 but excluding IE7&IE8). It is intended for installation on a system that has Service Pack 2 installed.

Installation can take up to 2 hours 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 CPSECPEP016S 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, 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 is resolved in CP5.0 SU04 and later).

3.1. List of WIs that are fixed by this PEP

wi01102418 New Security PEP needed for CallPilot Servers

Other fixes resolved in the replaced PEP:

wi01055706 Unable to install CPSECPEP015S unless previous SU has been installed
wi00858836 New Security PEP needed for CallPilot Servers
Q01367189 Excessive TCP Keep-Alive LAN traffic with Desktop Messaging
Q01449531 DMI view update sets CP services 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 server joined to Domain
Q01819279 Some registries are not added as expected
Q01830619 Wrong sevice name in readme.txt (TrkSrv)
Q01973128 CPSECPEP011S fails to install on 202i
Q01980200 Application popup after installation of CPSECPEP011S
Q02094497 Microsoft Base Security Analyzer fails after installing CPSECPEP011S
Q02116123 DCOM errors EVENT ID: 10020
Q02133709 DCOM Events10005 is generated after each reboot

3.2. List of hotfixes to patch the following Microsoft Bulletins

Bulletin	Date	KB number	Problem description
MS13-063	13.08.2013	2859537	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2859537)
MS13-062	13.08.2013	2849470	Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)
MS13-060	13.08.2013	2850869	Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2850869)
MS13-059	13.08.2013	2862772	Cumulative Security Update for Internet Explorer (2862772)
MS13-057	09.07.2013	2803821	Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (2847883)
MS13-056	09.07.2013	2845187	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2845187)
MS13-054	09.07.2013	2834886	Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)
MS13-053	09.07.2013	2850851	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)
MS13-052	09.07.2013	2833949	Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)
MS13-033	09.04.2013	2820917	Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2820917)
MS13-027	12.03.2013	2807986	Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)
MS13-011	12.02.2013	2780091	Vulnerability in Media Decompression Could Allow Remote Code Execution (2780091)
MS13-010	12.02.2013	2797052	Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2797052)
MS13-004	08.01.2013	2742604	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324)
MS13-002	08.01.2013	2758694, 2758696	Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)
MS12-082	11.12.2012	2770660	Vulnerability in DirectPlay Could Allow Remote Code Execution (2770660)
MS12-081	11.12.2012	2758857	Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)
MS12-078	11.12.2012	2753842	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)
MS12-072	13.11.2012	2727528	Vulnerabilities in Windows Shell Could Allow Remote Code Execution (2727528)

MS12-054	14.08.2012	2705219, 2712808	Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)
MS12-049	10.07.2012	2655992	Vulnerability in TLS Could Allow Information Disclosure (2655992)
MS12-048	10.07.2012	2691442	Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)
MS12-045	10.07.2012	2698365	Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)
MS12-043	10.07.2012	2719985	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)
MS12-038	12.06.2012	2686828	Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)
MS12-036	12.06.2012	2685939	Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)
MS12-035	08.05.2012	2604092	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)
MS12-034	08.05.2012	2659262, 2676562, 2686509	Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)
MS12-025	12.06.2012	2656369	Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)
MS12-024	10.04.2012	2653956	Vulnerability in Windows Could Allow Remote Code Execution (2653956)
MS12-009	14.02.2012	2645640	Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)
MS12-006	10.01.2012	2638806	Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)
MS12-005	10.01.2012	2584146	Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)
MS12-004	10.01.2012	2598479, 2631813	Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)
MS12-002	10.01.2012	2603381	Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)
MS12-001	10.01.2012	2644615	Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)
MS11-100	30.12.2011	2656352, 2656358	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)
MS11-097	13.12.2011	2620712	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712)
MS11-093	13.12.2011	2624667	Vulnerability in OLE Could Allow Remote Code Execution (2624667)
MS11-090	13.12.2011	2618451	Cumulative Security Update of ActiveX Kill Bits (2618451)
MS11-075	11.10.2011	2564958	Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)
MS11-071	13.09.2011	2570947	Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)
MS11-062	09.08.2011	2566454	Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454)
MS11-043	14.06.2011	2536276	Vulnerability in SMB Client Could Allow Remote Code Execution (2536276)
MS11-042	14.06.2011	2535512	Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512)
MS11-038	14.06.2011	2476490	Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490)
MS11-037	08.11.2011	2544893	Vulnerability in MHTML Could Allow Information Disclosure

			(2544893)
MS11-033	12.04.2011	2485663	Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2485663)
MS11-031	12.04.2011	2510587	Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666)
MS11-030	12.04.2011	2509553	Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)
MS11-024	12.04.2011	2506212	Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)
MS11-020	12.04.2011	2508429	Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)
MS11-014	08.02.2011	2478960	Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege (2478960)
MS11-013	08.02.2011	2478971	Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)
MS11-011	08.02.2011	2393802	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)
MS11-006	08.02.2011	2483185	Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)
MS11-002	11.01.2011	2419635	Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)
MS10-101	14.12.2010	2207559	Vulnerability in Windows Netlogon Service Could Allow Denial of Service (2207559)
MS10-099	14.12.2010	2440591	Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege (2440591)
MS10-097	14.12.2010	2443105	Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)
MS10-096	14.12.2010	2423089	Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)
MS10-083	12.10.2010	979687	Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)
MS10-082	12.10.2010	2378111	Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)
MS10-081	12.10.2010	2296011	Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)
MS10-076	12.10.2010	982132	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)
MS10-074	12.10.2010	2387149	Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)
MS10-065	14.09.2010	2124261	Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)
MS10-062	14.09.2010	975558	Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (975558)
MS10-061	14.09.2010	2347290	Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)
MS10-052	10.08.2010	2115168	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)
MS10-042	13.07.2010	2229593	Vulnerability in Help and Support Center Could Allow Remote Code Execution
MS10-041	30.06.2010	979907	Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343)
MS10-040	30.06.2010	982666	Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)

MS10-033	23.06.2010	978695, 979482	Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)
MS10-029	21.04.2010	978338	Vulnerability in Windows ISATAP Component Could Allow Spoofing (978338)
MS10-026	22.06.2010	977816	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)
MS10-020	26.05.2010	980232	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)
MS10-019	21.04.2010	979309	Vulnerabilities in Windows Could Allow Remote Code Execution (981210)
MS10-013	10.02.2010	977914, 975560	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)
MS10-007	09.02.2010	975713	Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)
MS10-005	10.02.2010	978706	Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706)
MS10-001	12.01.2010	972270	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)
MS09-073	27.01.2010	973904	Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution (975539)
MS09-071	09.12.2009	974318	Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)
MS09-069	08.12.2009	974392	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)
MS09-059	14.10.2009	975467	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467)
MS09-057	13.10.2009	969059	Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)
MS09-056	14.10.2009	974571	Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)
MS09-053	13.10.2009	975254	Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)
MS09-052	13.10.2009	974112	Vulnerability in Windows Media Player Could Allow Remote Code Execution (974112)
MS09-051	13.10.2009	954155, 975025	Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682)
MS09-048	08.09.2009	967723	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)
MS09-046	08.09.2009	956844	Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)
MS09-044	25.08.2009	958469	Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927)
MS09-042	12.08.2009	960859	Vulnerability in Telnet Could Allow Remote Code Execution (960859)
MS09-041	11.08.2009	971657	Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657)
MS09-040	11.08.2009	971032	Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032)

MS09-037	11.08.2009	973869, 973507, 973815, 973540, 973354	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)
MS09-020	17.06.2009	970483	Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)
MS09-015	15.04.2009	959426	Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)
MS09-013	14.04.2009	960803	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)
MS09-012	14.04.2009	952004, 956572	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)
MS09-010	14.04.2009	923561	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)
MS08-076	09.12.2008	952069	Vulnerabilities in Windows Media Components Could Allow Remote Code Execution
MS08-071	09.12.2008	956802	Vulnerabilities in GDI Could Allow Remote Code Execution
MS08-062	14.10.2008	953155	Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution (953155)
MS08-049	12.08.2008	950974	Vulnerabilities in Event System Could Allow Remote Code Execution (950974)
MS08-048	12.08.2008	951066	Security Update for Outlook Express and Windows Mail (951066)
MS08-046	12.08.2008	952954	Vulnerability in MS Windows Image Color Management System Could Allow RCE (952954)
MS08-038	08.07.2008	950582	Vulnerability in Windows Explorer could allow remote code execution
MS08-036	10.06.2008	950762	Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762)
MS08-022	08.04.2008	944338	Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution (944338)
MS08-007	12.02.2008	946026	Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)
MS08-005	12.02.2008	942831	Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)
MS07-068	11.12.2007	941569	Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275)
MS07-067	11.12.2007	944653	Vulnerability in Macrovision Driver Could Allow Elevation of Privilege (944653)
MS07-061	13.11.2007	943460	Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460)
MS07-050	14.08.2007	938127	Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)
MS07-040	10.07.2007	933854	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)
MS07-039	10.07.2007	926122	Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)
MS07-034	12.06.2007	929123	Cumulative Security Update for Outlook Express and Windows Mail (929123)
MS07-028	08.05.2007	931906	Vulnerability in CAPICOM Could Allow Remote Code Execution (931906)
MS07-020	10.04.2007	932168	Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)

MS07-017	03.04.2007	925902	Vulnerabilities in GDI Could Allow Remote Code Execution (925902)
MS06-078	12.12.2006, 07.10.2007	923689, 925398	Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689)

KB890830	Windows Malicious Software Removal Tool V5.3
KB927891	Update for Windows Installer (MSI)
KB942840	Update for Windows Server 2003 (KB942840)
KB936357	A microcode reliability update is available that improves the reliability of systems that use Intel processors
KB968389	Update to help strengthen authentication credentials in specific scenarios
KB967715	Update to resolve an issue in which AutoRun features were not correctly disabled
KB 973917	Update that implements Extended Protection for Authentication in Internet Information Services (IIS)
KB 973688	Update for Microsoft XML Core Services 4.0 Service Pack 2
KB 973687	Updates for Microsoft MSXML Core Services 3.0 and MSXML Core Services 6.0
KB 973686	Update for MSXML Core Services 6.0 Service Pack 2
KB 971737	Description of the update that implements Extended Protection for Authentication in Microsoft Windows HTTP Services (WinHTTP)
KB 955759	Microsoft Security Advisory: Description of the AppCompat update for Indeo codec
KB971029	Update to the AutoPlay functionality in Windows
KB957579	Post-installation behavior on client computers after you install the DNS update
KB2524375	Update to resolve an issue which requires an update to the certificate revocation list on Windows systems and to keep your systems certificate list up to date
KB2562937	Update Rollup for ActiveX Kill Bits
KB2616676	Fraudulent Digital Certificates Could Allow Spoofing
KB2718704	Cumulative Security Update for ActiveX Kill Bits
KB2728973	Unauthorized digital certificates could allow spoofing
KB2661254	Update for minimum certificate key length
KB2736233	Update Rollup for ActiveX Killbits
KB2749655	Compatibility issues affecting signed Microsoft binaries
KB2748349	Corrupted files are found in backup data that is restored by using the Windows Volume Shadow Copy feature
KB2798897	Unauthorized digital certificates could allow spoofing
KB2808679	Update that protects from internal URL port scanning
KB2820197	Update Rollup for ActiveX Killbits

3.3. Changing 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 as 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)
- MS08-008: Disable attempts to instantiate Microsoft Forms 2.0 ImageActiveX Control in IE
- MS08-010: 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
- RealPlayer ActiveX vulnerability Workarounds: Set killbits for rmoc3260.dll version 6.0.10.45 (KB240797)
- Close off some unneeded TCP ports by using an IP Security policy (1027, 1031, 1033 and 2019)
- Disable JavaScript in Adobe Reader PDF files for the Administrator userid (workaround for multiple security vulnerabilities reported November 2008)
- Improved disabling of the AutoRun on all drives
- Uninstall unneeded Java Runtime Engine 1.3.1-11 from some CP Servers
- Changed permissions on disabled services
- Added more auditing to disabled services
- Changed Audit Policy - Audit privilege use from Success&Fail to Failure only
- Network Access Remotely accessible registry paths and subpaths
- Network Security: LAN manager authentication level
- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
- User Rights: Deny logon as a batch job
- User Rights: Deny logon through Terminal Services
- Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
- System objects: Default owner for objects created by members of the Administrators group
- Remote Administration Service set to Disabled
- Security Log: Maximum Event log size changed from 16384KB to 81920KB
- MSS MinimumDynamicBacklog changed to 20 from 10
- File Permissions tightened for several files
- Autorun: HonorAutorun setting registry value set
- IE hardening and zone settings updated
- IIS6 Installation, several settings updated
- Restrict permissions on some system tools
- Audit failures for the Everyone group for all files/folders on the system drive
- Set permissions for all DCOM objects to Administrators F, System F, Users R

- Ensure policies are reprocessed even if Group Policy objects have not changed
- Protect against Office Web Components vulnerability KB973472
- Disable parsing of Quicktime files
- Disallow anonymous SID/Name translation
- Adobe Reader disallow opening non-PDF file attachments with external applications
- Remove keys related to Remote Administration Service DCOM to fix event 10005 on reboot
- Java JRE javaws vulnerability - set kill bit
- Prevent Windows Media Player ActiveX control from running in IE (MS10-027 workaround)
- Disable HCP protocol
- MS10-071 - set kill bit for CVE-2010-3329
- Disable MP3 audio codec usage
- Disable MPEG Layer-3 parsing in DirectShow
- Disable FTP bounce attack
- Disable auto creation of administrative shares
- Disable AutoRestartShell to force the user to log out and log back in if a shell component crashes
- Adjust file permissions on C:\Windows\Repair
- Disable the ASP.NET ISAPI mapping
- Tighten file permissions on Wscript.exe and Cscript.exe

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)
- Automatic Updates (wuauserv)
- ClipBook (ClipSrv)
- DHCP Client (DHCP)
- Distributed File System (Dfs)
- Distributed Link Tracking Client (TrkWks)
- Distributed Link Tracking Server (TrkSvr)
- Error Reporting Service (ERSvc)
- File Replication (NtFrs)
- Help And Support (helpsvc)
- 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)
- Web Element Manager (elementmgr)
- 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 service is set to manual in order to reduce the attack surface

- Logical Disk Manager (dmserver)

4. Pre-installation notes

a). Make sure you are installing this PEP on a CallPilot 3.0, 4.0, 5.0 or 5.1 server

This PEP replaces the following PEPs if applicable:

- ✓ CP300SEC002S
- ✓ CP303SEC003S
- ✓ CP303SEC004S
- ✓ CP303SEC005S
- ✓ CP404SEC003S
- ✓ CP404SEC004S
- ✓ CP404SEC005S
- ✓ CPSECPEP006S
- ✓ CPSECPEP007S
- ✓ CPSECPEP008S
- ✓ CPSECPEP009S
- ✓ CPSECPEP010S
- ✓ CPSECPEP011S
- ✓ CPSECPEP012S
- ✓ CPSECPEP013S
- ✓ CPSECPEP014S
- ✓ CPSECPEP015S

The replaced PEPs will be automatically removed from DMI Viewer when CPSECPEP016S 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 about 750 MB on C: to start installation process, actual final disk space consumption is less than 270 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 CPSECPEP016S 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 CPSECPEP016S install to 520 MB.

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

-If Anti-Virus is installed, verify it is installed per the latest version of the bulletin entitled "CallPilot Support for Anti-virus Applications" (current number is P-2009-0039-Global). In particular, for CP4 systems, 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\CPSECPEP016S 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 CPSECPEP016S 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.

f). Since Service Pack 1 is not built into CallPilot 3.0 GA systems, PEP CP303SECSP1S needs to be used to install Service Pack 1 prior to installing CPSECPEPSP2S on a CP3 system. SP1 is already built in to CallPilot 4.0 and 5.0 GA systems. PEP CPSECPEPSP2S should be used to install SP2 on a CallPilot 3.0, 4.0, 5.0 or 5.1 system.

How to identify that Service Pack 2 has already been installed on your system: Open DMI Viewer or Add/Remove Program Applet. Please find CPSECPEPSP2S record. If CPSECPEPSP2S record exists then Service Pack 2 is installed on your system and you can continue with installation of CPSECPEP016S.

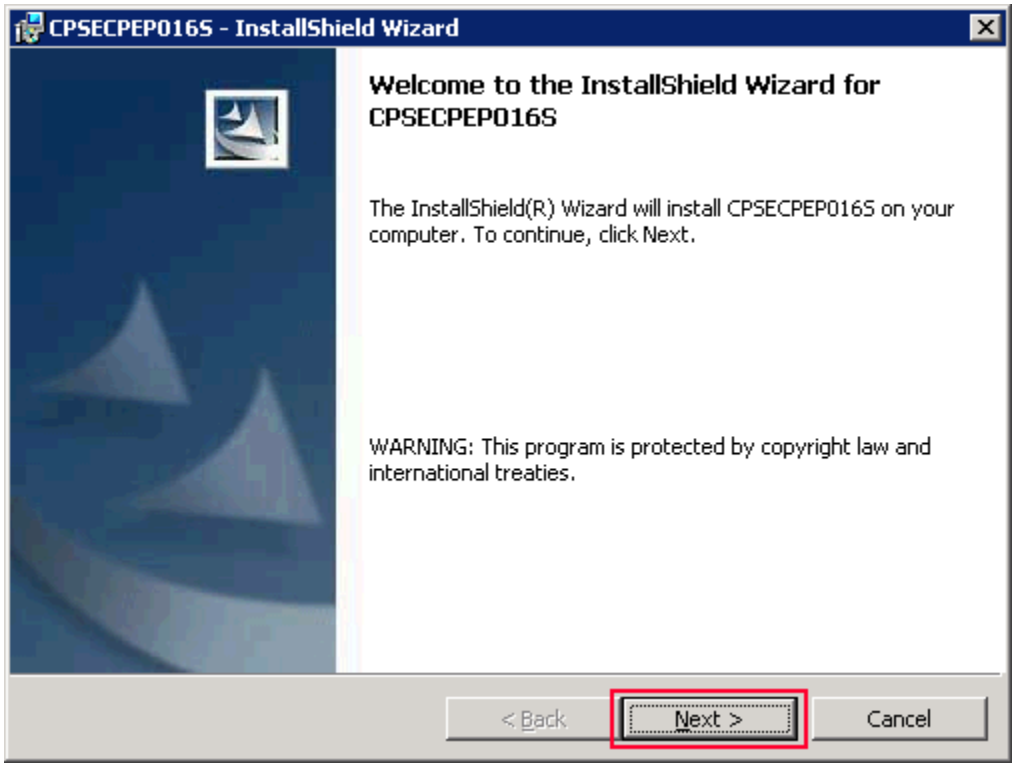
Special note for 202i and 1006r platforms: Service Pack 2 is installed with CallPilot 5.0 GA system on 202i and 1006r platforms. Therefore you can continue with installation of CPSECPEP016S on 202i and 1006r platform.

5. Installing the PEP

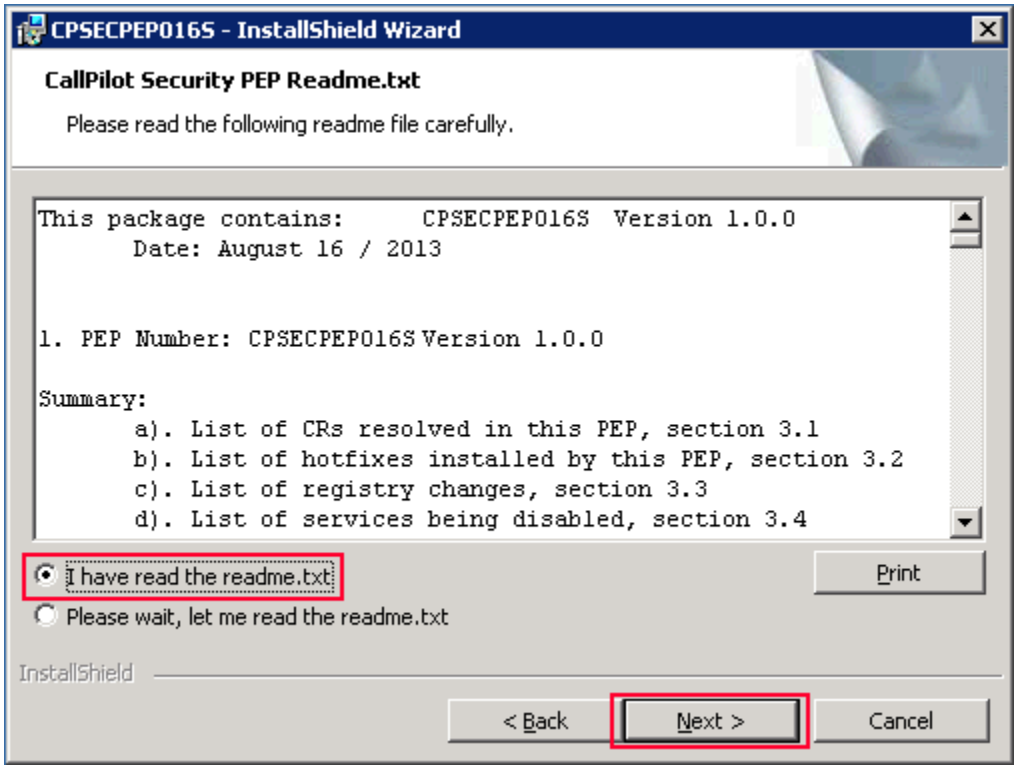
NOTE FOR INSTALLING ON HIGH AVAILABILITY SERVERS:
CallPilot security PEPs do not impact either the database or the MMFS. This is also true for the installation of Microsoft hotfixes directly. Therefore it is possible to install security PEPs and MS hotfixes on the standby server. In order to minimize downtime, the following procedure is recommended (assumes CP1 is initially active, CP2 is initially standby)

1) Install the security PEP (or hotfix) on the CP2 and reboot CP2
2) Once CP2 is fully rebooted, switch the CallPilot resource group to from CP1 to CP2
3) Install the security PEP (or hotfix) on CP1 and reboot CP1
4) Once CP1 is fully rebooted, if desired, switch the CallPilot resource group back to CP1

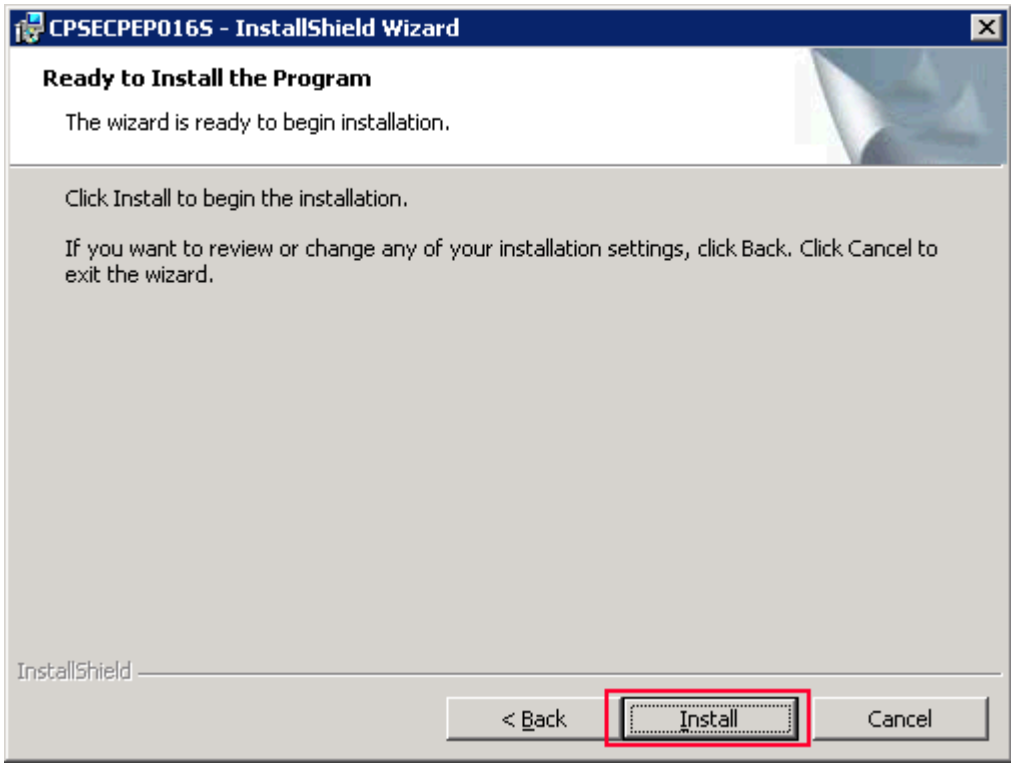
a). Begin installation by double-clicking on CPSECPEP016S.msi
NOTE: If you run the MSI from a network location (e.g. a shared network drive), you will get an "Open File Security Warning" window asking that "Are you sure you want to run this software?" just click on the Run button to run it.



b). Click on Next button on window "Welcome to the InstallShield Wizard for CPSECPEP016S" and continue on to the Readme window.

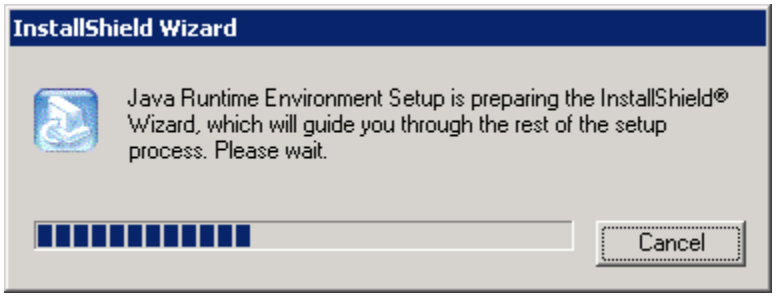


After reading through the readme, select Radio Button "I have read the readme.txt" and click on Next button.

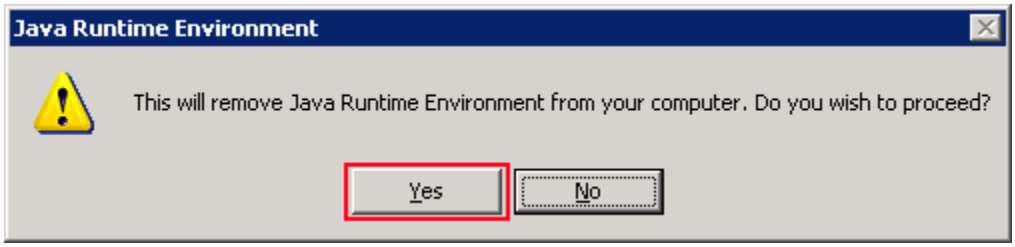


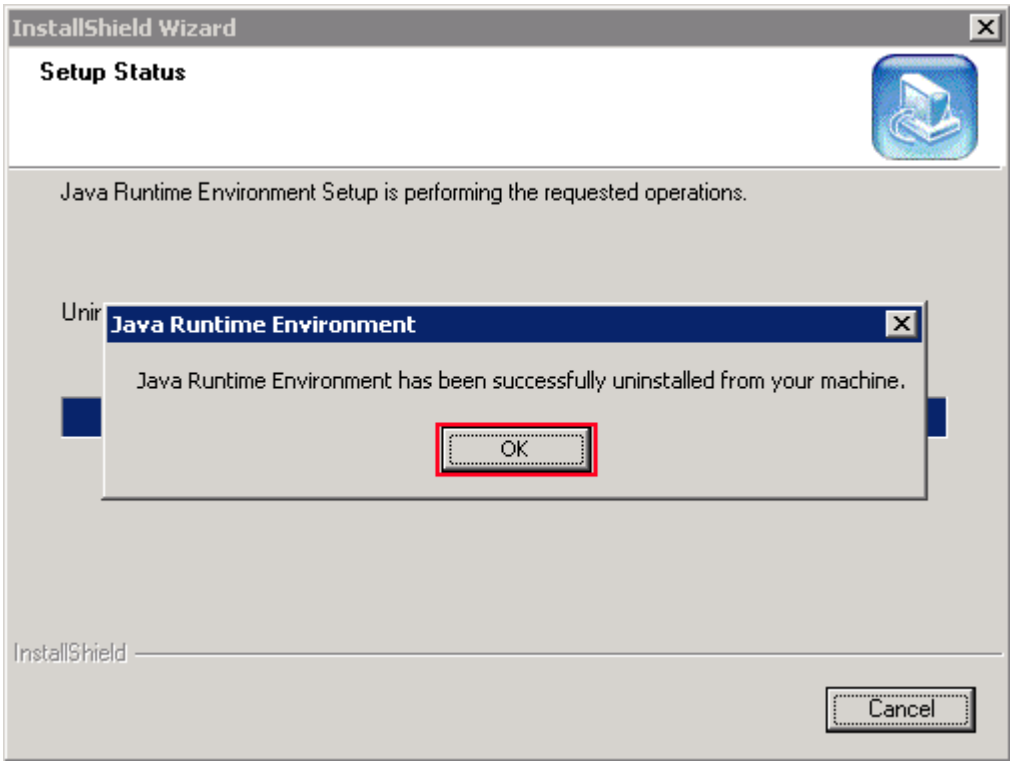
On next window "Ready to install the Program", click on Install button to install.

NOTE: Some cases, PEP will uninstall unneeded Java Runtime Environment. In this case, you will receive pop-up windows about it.

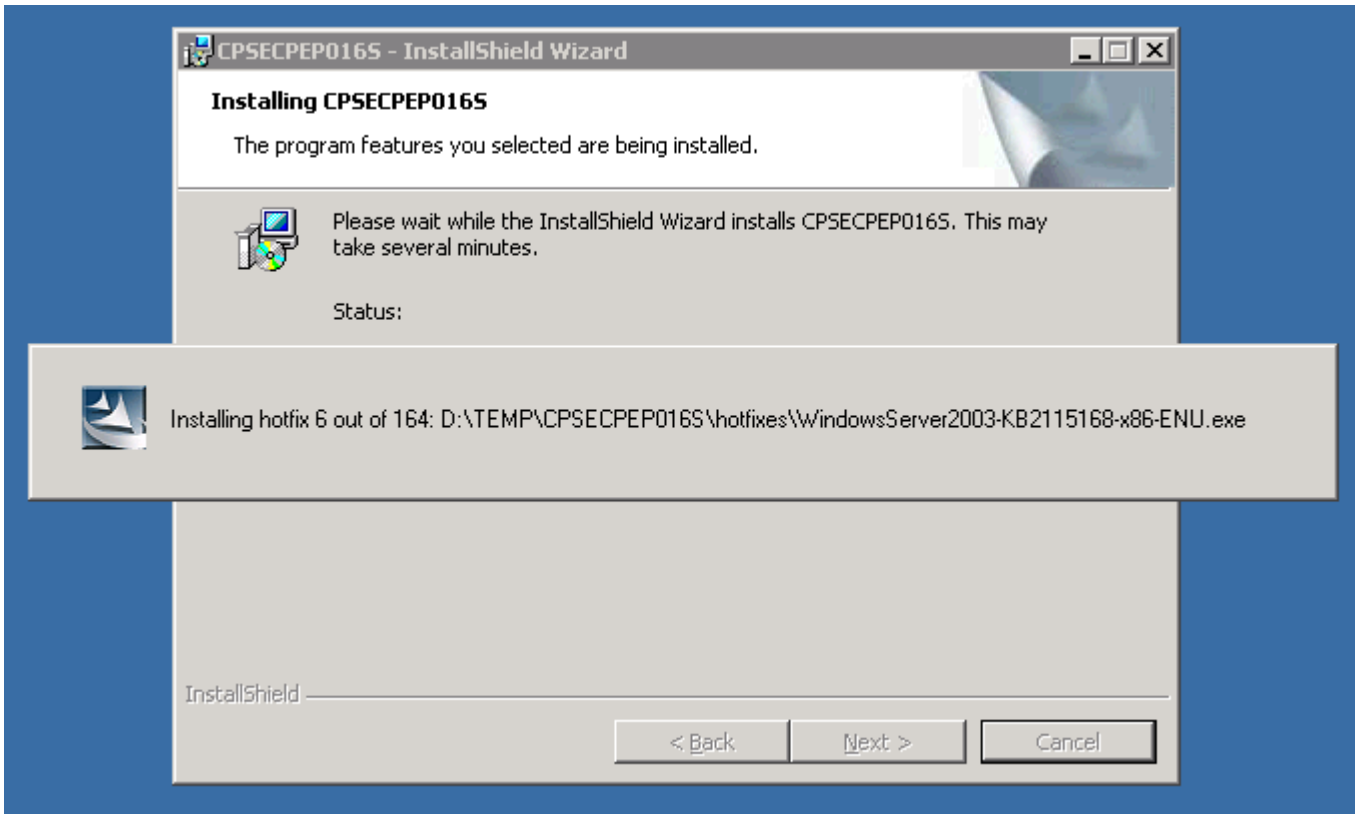


Please click "Yes" and "OK" when prompted.





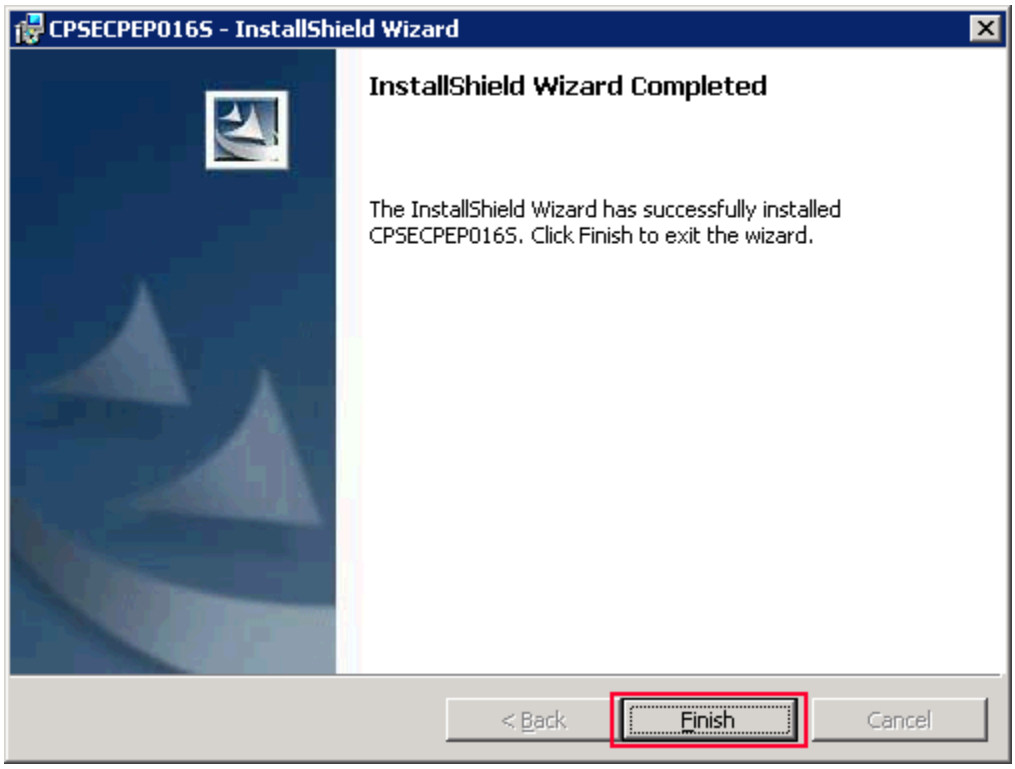
In other cases, just continue installation as usual.



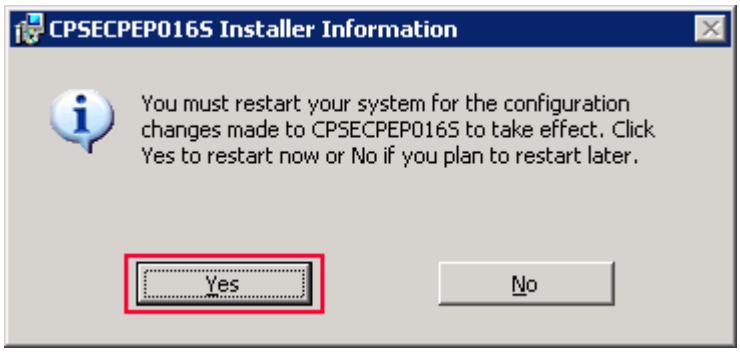
NOTE: Some cases, the main installation window "Installing CPSECPEP016S" will show up in front of the message box "Installing Hotfixes", that is a glitch of InstallShield, you may click on the message box and bring it to the front, either way will NOT affect the PEP install process.

NOTE: Total time required will be about 60 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 saying "InstallShield Wizard Completed". Click on the "Finish" button to exit the wizard, and then you will be prompted to "Click Yes to restart now or No if you plan to restart later". You need to restart the system for the 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.

e). After this PEP has been installed, the first time Internet Explorer is launched, a popup may been seen "Internet Explorer is not the default browser". Simply click to set it to be the default browser. Also, an event log may be seen about the Print Spooler not running when a remote desktop session is established. This event can be ignored.

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 CPSECPEP016S in DMIViewer will 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 (DMI Viewer), 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 hotfix checker:
Double-click D:\TEMP\CPSECPEP016S\Checker\CheckHotFixes.bat

NOTE: You also may use the following method to run Checker:
In the Start menu select "Start" > "Run..." command. Run dialog appears.
Type "D:\TEMP\CPSECPEP016S\Checker\CheckHotFixes.bat" (without quotes) or
"D:\TEMP\CPSECPEP016S\Checker\CheckHotFixes.bat current" (without quotes) and press [OK].

NOTE: You may use CheckHotFixes.bat with the "current" parameter to check against the current hotfix list, i.e. a hotfix list downloaded dynamically from Microsoft. This method requires internet connection to work properly. Without the "current" parameter script checks against a hotfix list that was current when the PEP was released. Internet connection is not required in this case.

NOTE: Verifying hotfixes can take up to 20 minutes depending on your platform and CallPilot release.

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.

NOTE: Probably some hotfixes from the following list will be shown as missed updates:

- Windows Internet Explorer 7 for Windows Server 2003
- Windows Internet Explorer 8 for Windows Server 2003
- Daylight Savings time change (KB2863058)
- Microsoft .NET Framework 2.0, 3.5 and 3.5.1 updates on HA systems

It is normal for this PEP. On HA systems, the missing .NET updates must be installed separately.