NORTEL NETWORKS

Product Bulletin

Number: 2002-087

Date: May 24, 2002

CallPilot 1.07 Server Security Update

Nortel Networks announces the release of the CallPilot 1.07 Server Security Update PEP NM010709G078S (78S), effective May 24, 2002. Installation of this server update results in increased security of the CallPilot server by providing all applicable Microsoft Operating System updates and enhancements in an easy to implement PEP. This bulletin outlines the recommended actions, ordering information, and an overview of the installation process. For a detailed listing of all updates, refer to Appendix-A.

Recommended Action

The Server Security Update PEP, NM010709G078S, should be applied during the next maintenance activity to all CallPilot 1.07 servers that have been installed with or upgraded to CallPilot 1.07, Service Update 4 (SU-4).

To install this update follow the readme.txt file included with the PEP, or the instructions as outlined in Appendix-B. The server will be rebooted automatically several times during the installation process.

Hardware/Software Affected

This server update is only applicable to CallPilot 1.07 servers that have been installed with, or upgraded to CallPilot 1.07, Service Update 4 (SU-4).

Documentation Codes

No Documentation changes have resulted from this update

Order Codes

No Order Code changes have resulted from this update.

Ordering Information

The CallPilot Server Security Update PEP may be obtained two different ways:

- Order NTZE60AA to obtain the complete Service Update PEP CD kit. This CD kit includes all the latest Service Updates for CallPilot 1.07. Effective June 24, 2002, all new orders for this update include the revised Server PEP CD that includes PEP NM010709G078S (78S).
- Order NTUB43AC / A0805372 for the individual CallPilot 1.07 Server PEP CD version 1.07.09.15. Effective June 24, 2002, all new orders for this CD will receive this latest version.
- Download the PEP from the Meridian PEP Library (MPL) website at the following URLs:

  North America: https://www43.nortelnetworks.com/MPL
  Europe, Middle East, and Africa: https://www21.nortelnetworks.com/MPL

  Notes:
  1. A secure user-ID/password is required for access to this site.
  2. This PEP is 107MB in size.

Appendix-A

The following list outlines the specific changes and enhancements contained within the CallPilot Server Security Update PEP NM010709G078S (78S). While this update primarily consists of Microsoft hot-fixes, please note that only those hot-fixes that were deemed applicable to CallPilot servers are included. No other Microsoft hot-fixes should be applied to the server.

Security Update Details:

- Updates the server to Windows NT 4 Service Pack 6a
- Updates Internet Explorer to version 5.5 with Service Pack 2
- Converts the system drive (C or D, wherever Windows NT is located) to NTFS if not already
- Converts default SNMP start-up operation to “disabled“
- Applies the following Microsoft security roll-up packages and hot fixes (that may apply to CallPilot)
    - MS98-001 – Disable creation of local groups on domain by non-administrative users (creatals.exe)
    - MS99-041 – RASMAN Security Descriptor Vulnerability (fixrasi.exe)
    - MS00-079 – HyperTerminal Buffer Overflow Vulnerability (Q304158i.exe)
    - MS01-022 – WebDAV Service Provider Can Allow Scripts to Levy Requests as User (rbupdate.exe)
    - MS01-044 – File Fragment Reading via .HTR Vulnerability (frgvuli.exe)
    - MS01-048 – Malformed Request to RPC Endpoint Mapper (q305399i.exe)
    - MS01-056 – Windows Media Player .ASF Processor Unchecked Buffer and other cumulative patches (wm308567.exe and also includes MS01-042)
    - MS02-006 – Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run (Q314147i.exe)
    - MS02-009 – Incorrect VBScript Handling in IE can Allow Web Pages to Read Local Files (vbs55men.exe)
    - MS02-013 – Java VM: Java Applet Can Redirect Browser Traffic (msjavx86.exe and also includes MS00-081)
    - MS02-014 – Unchecked Buffer in Windows Shell Could Lead to Code Execution (Q313829i.exe)
    - MS02-017 – Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution (Q312895i.exe)
    - MS02-023 – Cumulative update for IE5.5/SP2 to address six new vulnerabilities (Q321232.exe)
    - Q299444i.exe - Security Rollup Package for NT4 and IIS4
- Applies two Symantec pcAnywhere 8 updates that are often overlooked from the documented NTP procedures.
- Updates the SCSI driver for 200i/201i platforms (reference Product Bulletin 2002-076)

Appendix-B

The following steps provide an overview of installing the CallPilot Server Security Update PEP, NM010709G078S. These guidelines are also summarized in the readme.txt file available with this PEP.

Notes:

1. Ensure that a useable, recent Full System backup is available. If not, it is recommended that one be performed prior to installing this update.

2. If any other changes requiring a reboot are to be done, please complete those activities and reboot the system to full service before applying this PEP. Attempting to combine several changes into a single reboot could result in a system that will not boot up and may require a re-install of the software.

3. The password to the Administrator account is temporarily changed to NULL so that the PEP installation process can automatically logon. At the end of the PEP installation, you will be prompted for a new Administrator password. It's recommended that a new Administrator password be selected for use before completing the installation of this PEP. It is also recommended that all passwords for all Windows NT Logon accounts have their passwords changed from their default values to new strong values selected by the customer. Those accounts are:
    a. Administrator
    b. NgenSys
    c. NGenDist
    d. NgenDesign
    e. Gamroot (only on systems using Mylex AR352 RAID Controller Card)

4. The SNMP service startup option will be disabled by default. Document whether or not SNMP monitoring is being used. If required re-enable the service after installing the PEP using Control Panel / Services and configure SNMP properly.

5. This PEP cannot be uninstalled. Attempting to uninstall the PEP will only remove the record of this update from the list of installed PEPs within DMIViewer, however the software changes themselves are not removed.

Installation Overview:

This PEP uses "Automatic Button Pushing" to perform some of the installation steps without any user interaction. It's important that the installer does not interfere with this. In some cases it may seem that nothing is happening for up to five (5) minutes. Please be patient. The PEP installation process is automatic. Once started, no interaction is required until about 40 minutes later where the system will prompt for the Administrator password.

In the event of a problem, if a particular screen cannot be automatically identified or located, pressing the "Retry" button may resume automatic control.

This PEP contains five separate sections (A, B, C, D, and E) that perform various portions of the update as follows:

Section-A

- Verify free disk space
- Shutdown all CallPilot services
- Change all CallPilot services startup to Manual mode
- Archive pcAnywhere configuration data and remove pcAnywhere application
- Install NT 4 Service Pack 6A and reboot

Section-B

- Upgrade Internet Explorer to IE5.5, apply Service Pack 2, and reboot

Section-C

- Re-install pcAnywhere, recovery configuration data, and apply associated patches
- Apply initial Microsoft hot-fixes and QChain.EXE for applying multiple security hot-fixes without intermediate reboots

Section-D

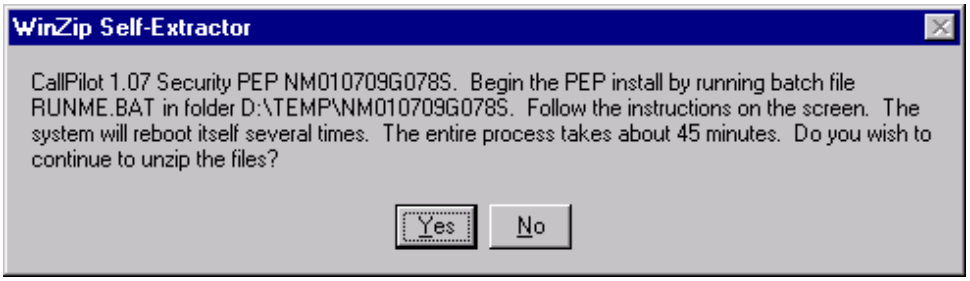
- Install remaining system patches

Section-E

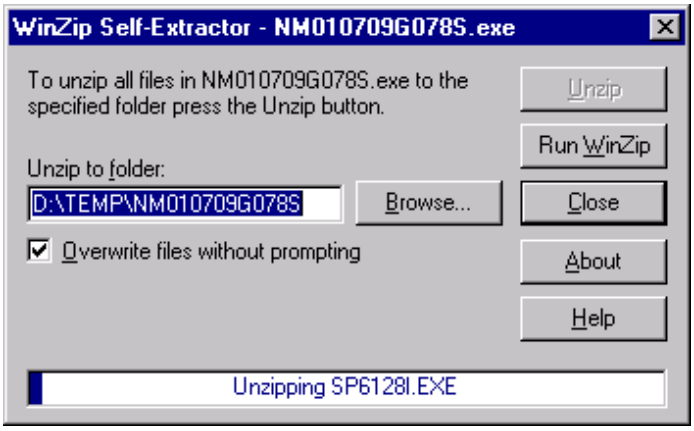
- Apply all Microsoft hot-fixes
- Change all CallPilot services startup back to Automatic mode
- Prompt/Change user for new Administrator Password
- Complete installation and reboot CallPilot to full service.

Installation Steps:

1. Double-click on PEP NM010709G078S.EXE. The following window will appear.



2. Click “Yes” to continue with unzipping the files. The “Self-Extractor” window will appear and extract all files to D:\TEMP\NM010709G078S. Once completed, the window will close automatically.



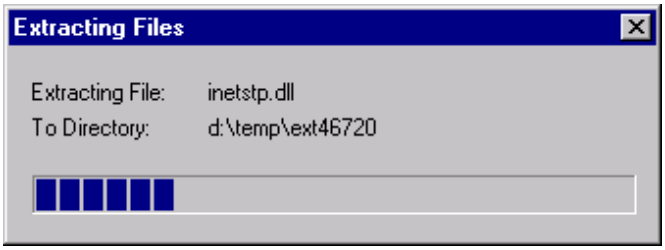
3. Using Explorer, navigate to folder D:\TEMP\NM010709G078S and double-click the RUNME.BAT file to begin the PEP installation. A “Read-Me First” pop-up notepad window will appear advising of the hot-fix updates to be applied and the required Administrator password change.

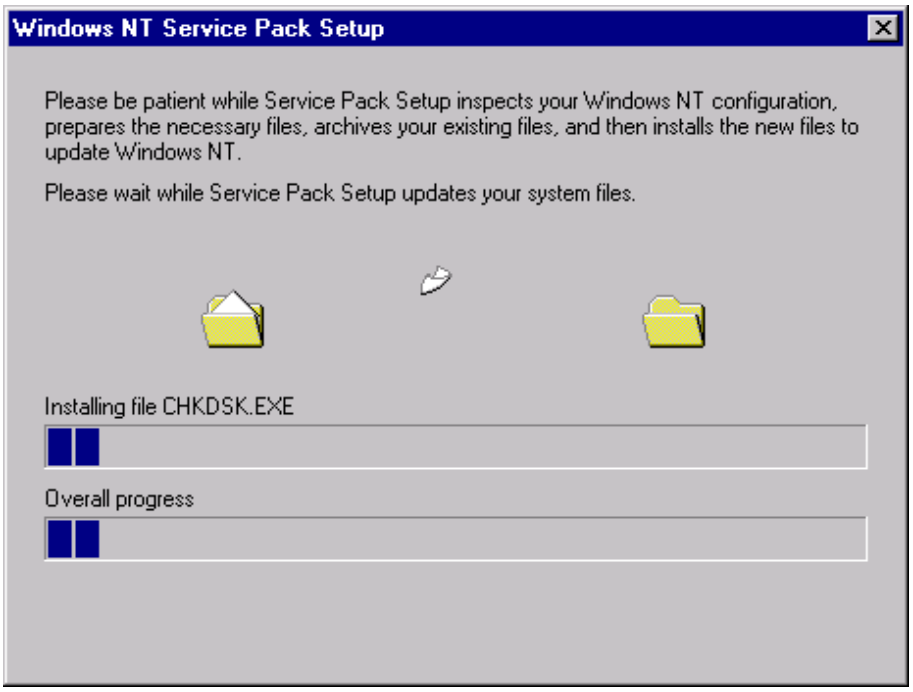
   To continue, exit out of Notepad. To cancel installation of this PEP, close the RUNME Command-prompt window.

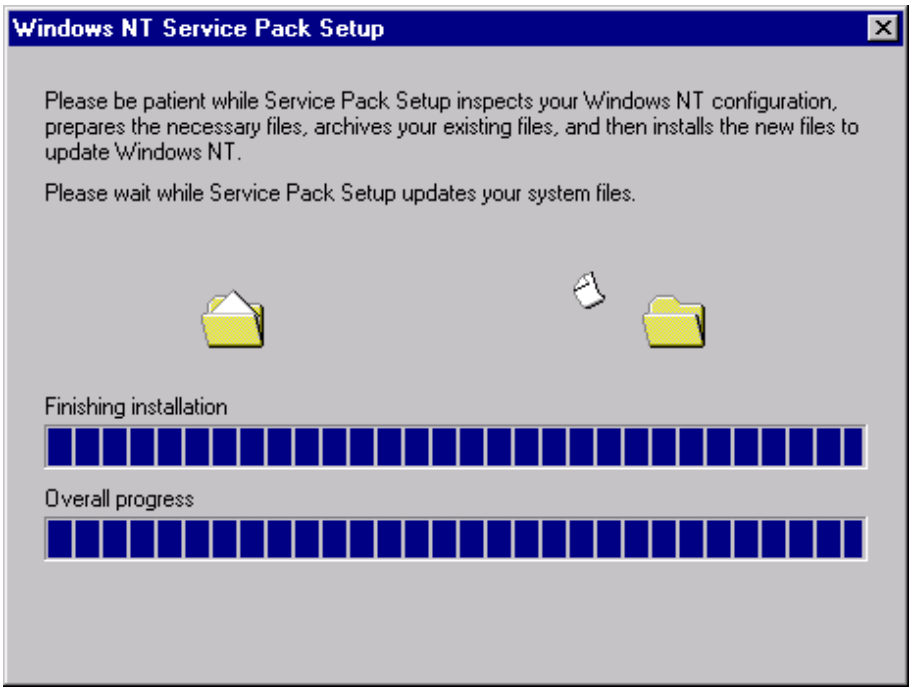
4. A new “Installer” window for Section-A will appear outlining the tasks that will be completed. As each step is begun, the text will change colors.

   At this point, **no further keyboard or mouse input should be required** for approximately 40 minutes where the system will prompt for the Administrator password. Allow each section to process and the reboots to complete automatically and without interaction.

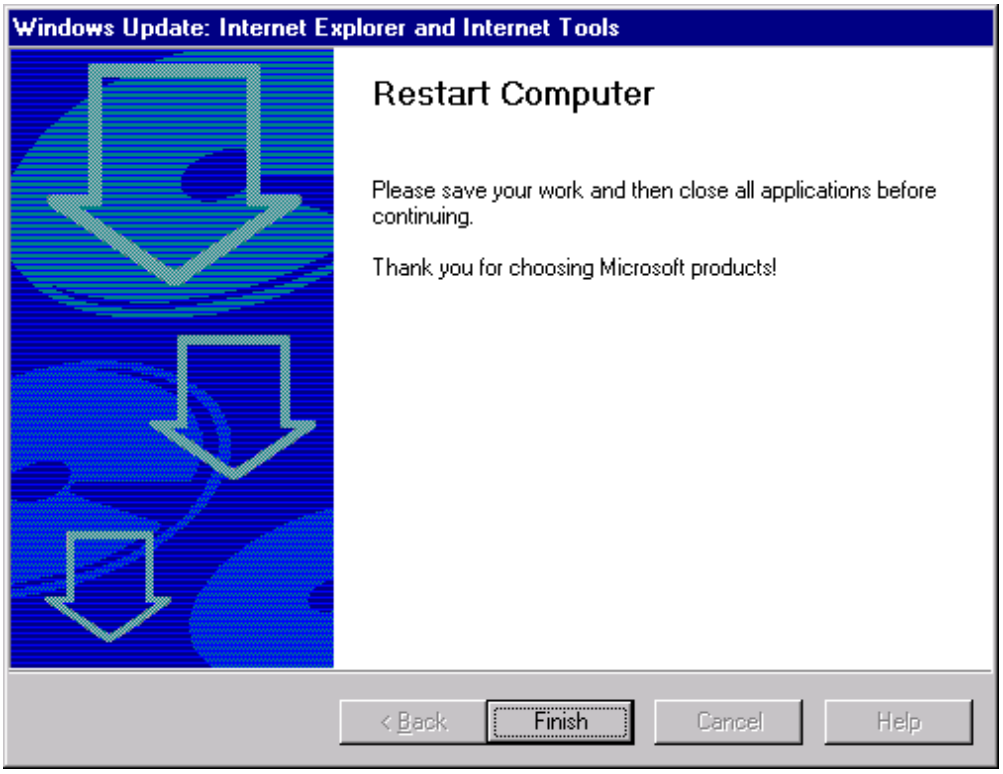
5. Once pcAnywhere has been uninstalled, the process continues with deleting any unnecessary files and then onto installing Windows NT Service Pack 6a. The following windows will appear:



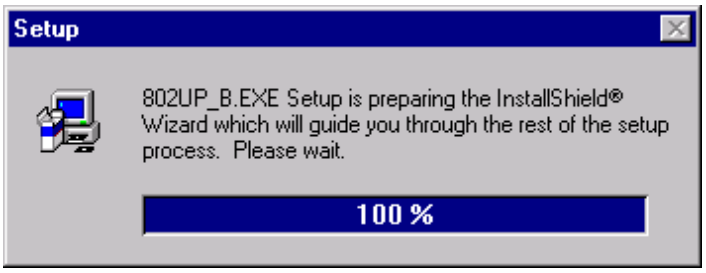




6. Once completed, the server will reboot and the automated process will continue with installing Internet Explorer 5.5 with Service Pack 2. Once IE5.5 is installed, the following window will appear and server will again reboot.



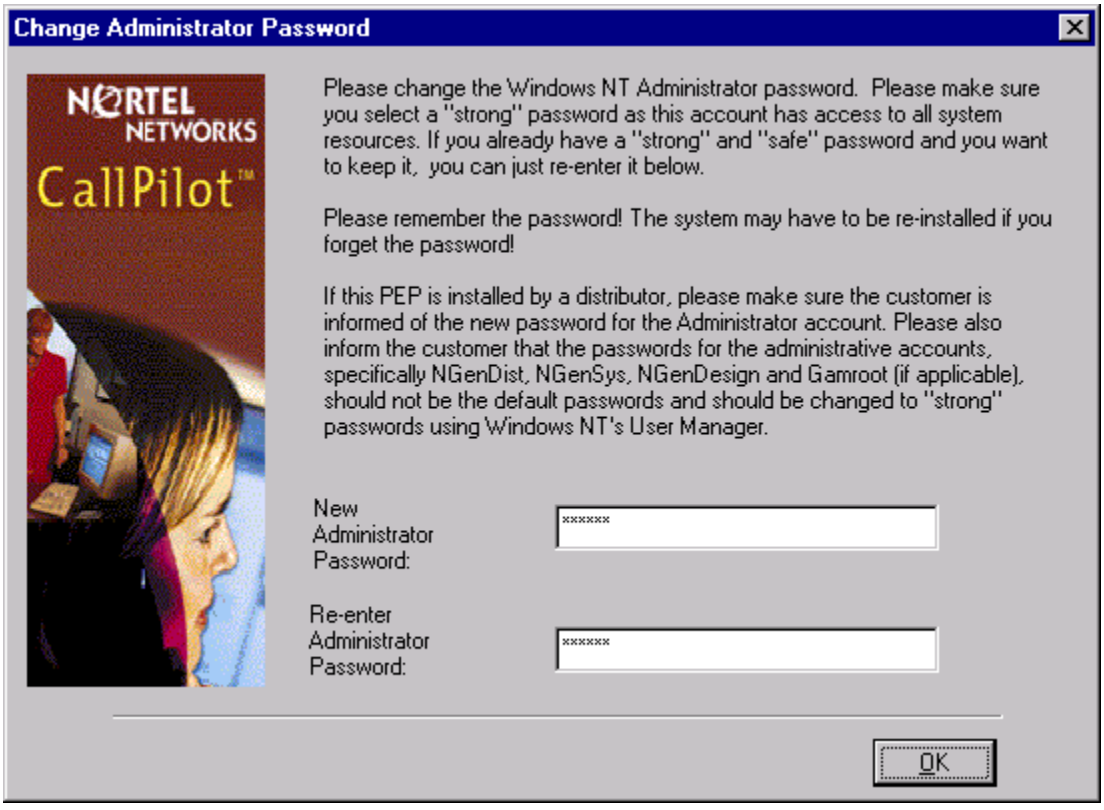
7. Upon reboot, pcAnywhere and its associated patches (802UP_A and 802UP_B) will be re-installed. Pop-up windows such as depicted below will appear.



The system will then proceed with applying the initial Microsoft hot-fixes and the QChain utility (for applying multiple hot-fixes without requiring intermediate reboots). The system will then reboot and continue to Section-D.

8. In Section-D, all system patches are applied and the process will continue to Section-E.

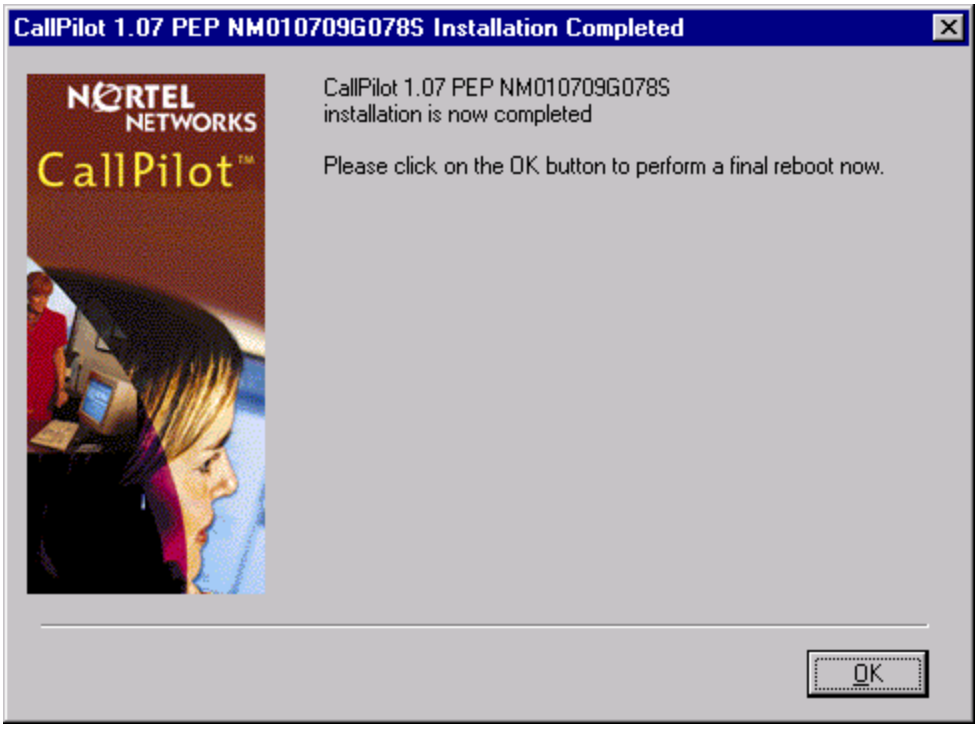
9. In Section-E, once application of all Microsoft hot-fixes has completed, the following window will appear prompting for the new Administrator Password.



10. At this point it is okay to again interact with the system using the keyboard and mouse.

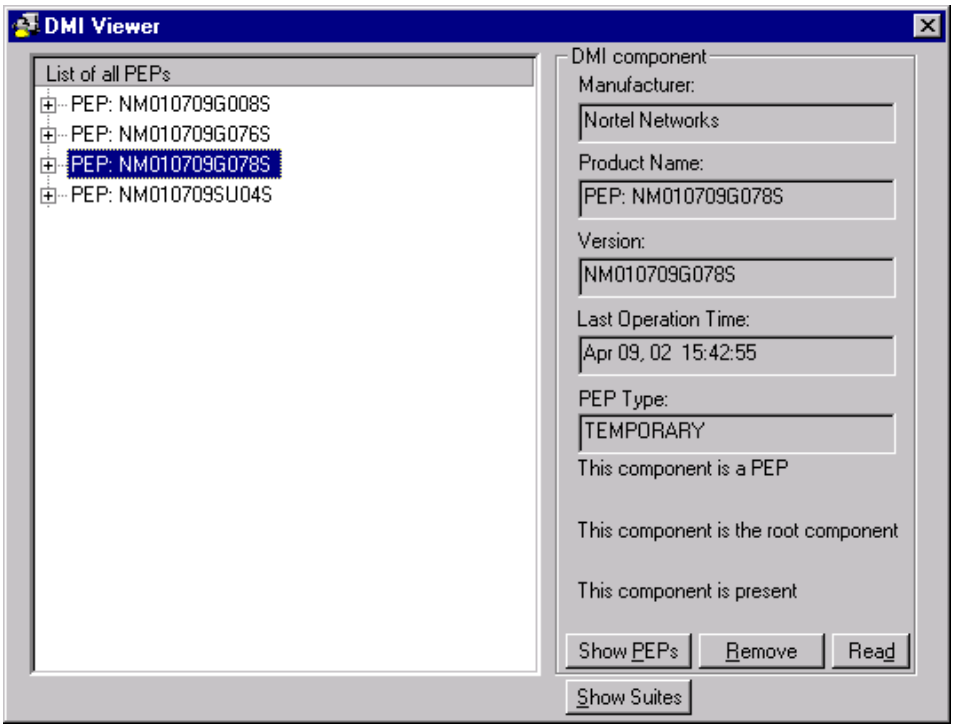
Enter the previous or a new Administrator Password and click “OK” to continue. It is recommended that a ‘strong’ and ‘secure’ password be used.

11. All CallPilot services will be setup to restart automatically and the following window will appear:



12. Press “OK” to perform a final reboot of the server. CallPilot will reboot to full service and installation of the PEP is complete.

13. Upon reboot, verify that PEP 78S is installed by using the DMIViewer. To launch the utility, choose Start > Programs > CallPilot > System Utilities > PEP Maintenance Utility. A sample of this screen is as follows:

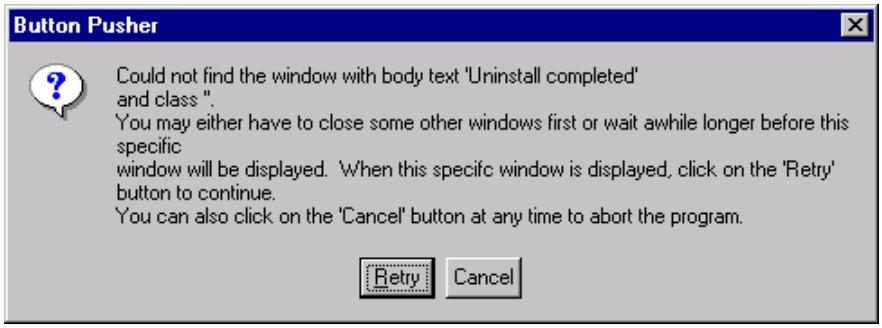


14. Delete any unused temporary files within C:\TEMP and D:\TEMP folders. Do not become alarmed if one or more files cannot be removed because they appear "Open". This condition will typically clear after the next reboot of the server.

15. Verify operation of pcAnywhere by establishing a remote session to the server.

16. If SNMP monitoring of the CallPilot server was originally implemented, the service will need to be modified to start up automatically. From Control Panel / Services, select the SNMP service and set the startup type to "Automatic".

    Note: If during the automated process the "Button Pusher" window appears (as depicted below), it's recommended to allow the system to attempt to locate the desired window and proceed on it's own.



    If for some reason, the requested window does not appear or has appeared but the PEP installation program hasn't detected it, click the "Retry" button. The installation program should locate the desired window and proceed automatically.

    If further assistance is required for installation of this PEP, contact your Nortel Networks support organization.