



# **Avaya CallPilot® Preventative Maintenance Guide**

5.0  
NN44200-505, 01.07  
December 2010

## Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

## Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

## Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

## Warranty

Avaya provides a limited warranty on its Hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

## Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

## Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

## Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

## Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

# Contents

<b>Chapter 1: New in this release.....</b>	<b>5</b>
Feature.....	5
Other changes.....	5
<b>Chapter 2: Customer service.....</b>	<b>7</b>
Getting technical documentation.....	7
Getting product training.....	7
Getting help from a distributor or reseller.....	7
Getting technical support from the Avaya Web site.....	8
<b>Chapter 3: Routine maintenance fundamentals.....</b>	<b>9</b>
Overview.....	9
Customer Documentation Map.....	9
Routine maintenance task checklists (daily, weekly, monthly, semi-annual).....	12
Daily routine maintenance tasks.....	13
Weekly routine maintenance tasks.....	13
Monthly routine maintenance tasks.....	14
Semi-annual routine maintenance tasks.....	15
Best practices for your site.....	15
Maintain a log book.....	15
Use only qualified technicians to work with the CallPilot system.....	16
Ensure recovery media is on-site.....	16
Ensure recovery hardware is on-site.....	17
Ensure no unauthorized third-party software is installed on the server.....	17
Do not surf the Internet on the CallPilot server.....	18
Log off the local Windows console when not in use.....	18
Do not apply customer-specific security hardening scripts to the CallPilot server.....	18
Safeguard your CallPilot passwords and change them periodically.....	19
Ensure remote access is operational.....	19
Ensure proper power and grounding.....	19
Ensuring all external cables are secured to their connectors.....	20
Ensure systems have a proper operating system certificate attached.....	20
Ensure the system is properly labeled.....	21
Follow recommended handling procedures when removing power from a 200 series server from the PBX shelf.....	21
<b>Chapter 4: Routine maintenance tasks: software and database maintenance.....</b>	<b>23</b>
Monitoring server performance and traffic.....	24
Monitoring event logs for Critical and Major events.....	24
Archiving Flight Recorder information.....	25
Viewing Flight Recorder archive statistics.....	26
Downloading Flight Recorder archives.....	26
Deleting Flight Recorder archives.....	26
Tip: Setting up an alarm mailbox so you are notified of alarms.....	27
Checking that all call and multimedia channels are in service and can answer calls.....	27
Monitoring traffic using CallPilot Reporter.....	29
Keeping your software up-to-date.....	30
Checking for and installing the latest server SUs and any required PEPs.....	30
Checking for and installing the latest switch PEPs, and checking dependency lists.....	31

Keeping antivirus software up to date.....	31
Maintaining adequate storage space.....	32
Checking the space available in MMFS volumes.....	32
Removing unused mailboxes.....	33
Maintaining up-to-date backups.....	34
Performing regular full system backups for disaster recovery.....	34
Maintaining archives of users, prompts, applications, and voice forms.....	35
Verifying that scheduled backups are successful.....	36
Rotating tapes.....	36
Checking the backup network share for adequate space.....	37
Keeping the system secure.....	37
Ensuring all approved Microsoft Security Updates are installed.....	38
Performing quick security checks on the server.....	38
<b>Chapter 5: Routine maintenance tasks: hardware maintenance.....</b>	<b>41</b>
General maintenance tasks.....	41
Monitoring available hard disk space.....	41
Monitoring the health of your hard disks.....	42
Checking LED/HEX displays for error indications.....	44
Monitoring event logs for Critical or Major events.....	45
Maintaining server parts and cabling connections.....	45
Checking fans and power supplies for proper operation.....	45
Cleaning fan filters.....	46
Cleaning tape drive heads.....	47
Maintaining RAID drives.....	47
Checking the status of RAID disk packs.....	47
Checking the consistency of RAID drives.....	48
Ensuring RAID audible alarm is enabled on 1002rp and 703t.....	49
Ensuring RAID audible alarm is enabled on the 1006r.....	50
Checking the hard drive for media errors using the RAID Windows software.....	50
<b>Index.....</b>	<b>53</b>

# Chapter 1: New in this release

The following sections detail what's new in *Avaya CallPilot® Preventive Maintenance Guide* (NN44200-505) for Service Update 9 of Release 5.0.

---

## Feature

This document includes information about the new Flight Recorder feature. The following sections have been added for this feature:

- [Archiving Flight Recorder information](#) on page 25
- [Viewing Flight Recorder archive statistics](#) on page 26
- [Downloading Flight Recorder archives](#) on page 26
- [Deleting Flight Recorder archives](#) on page 26

---

## Other changes

See the following section for information about changes that are not feature-related:

Date	Changes
April 2009	Avaya CallPilot 5.0, Standard 01.04 of the Preventative Maintenance Guide is up-issued to update information on Monitoring event logs for Critical and Major events.
January 2009	CallPilot 5.0, Standard 01.03 of the Preventative Maintenance Guide is issued for general release.
March 2008	CallPilot 5.0, Standard 01.02 of the Preventative Maintenance Guide is up-issued to correct Avaya Product bulletin P-2003-0151-Global to P-2007-0101-Global.

New in this release

<b>Date</b>	<b>Changes</b>
May 2007	CallPilot 5.0, Standard 01.01 of the Preventative Maintenance Guide is issued for general release.

# Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to [www.avaya.com](http://www.avaya.com) or go to one of the pages listed in the following sections.

## Navigation

- [Getting technical documentation](#) on page 7
- [Getting product training](#) on page 7
- [Getting help from a distributor or reseller](#) on page 7
- [Getting technical support from the Avaya Web site](#) on page 8

---

## Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to [www.avaya.com/support](http://www.avaya.com/support).

---

## Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at [www.avaya.com/support](http://www.avaya.com/support). From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

---

## Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

---

## Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at [www.avaya.com/support](http://www.avaya.com/support).

# Chapter 3: Routine maintenance fundamentals

---

## Overview

The Preventative Maintenance Guide provides routine maintenance guidelines and procedures for the Avaya CallPilot® system. This guide is intended for the administrators, technicians, and engineers who maintain the Avaya CallPilot server.

CallPilot systems are designed to run smoothly with little maintenance, and they are engineered to meet the full capacity of your site. It is good practice, however, to perform certain routine maintenance tasks to avoid problems that can affect server performance or cause the server to fail. The CallPilot software and hardware includes a number of useful tools and indicators to help you monitor your server performance quickly and easily. With these tools, and some other helpful techniques described in this guide, you can develop daily, weekly, monthly, and semi-annual preventative maintenance routines. Checklists are included in this guide to help you remember the tasks. The Preventative Maintenance Guide also includes a list of best practices for your site.

---

## Customer Documentation Map

The following diagram shows the overall organization and content of the CallPilot documentation suite.

**Table 1: CallPilot Customer Documentation Map**

Fundamentals
Avaya CallPilot® Fundamentals Guide (NN44200-100)
Avaya CallPilot® Library Listing (NN44200-117)
Planning and Engineering
Avaya CallPilot® Planning and Engineering Guide (NN44200-200)
Avaya CallPilot® Network Planning Guide (NN44200-201)

Avaya Communication Server 1000 Converging the Data Network with VoIP Fundamentals (NN43001-260)

Solution Integration Guide for Avaya Communication Server 1000/CallPilot®/NES Contact Center/Telephony Manager (NN49000-300)

#### Installation and Configuration

Avaya CallPilot® Upgrade and Platform Migration Guide (NN44200-400)

Avaya CallPilot® High Availability: Installation and Configuration (NN44200-311)

Avaya CallPilot® Geographic Redundancy Application Guide (NN44200-322)

Avaya CallPilot® Installation and Configuration Task List Guide (NN44200-306)

Avaya CallPilot® Quickstart Guide (NN44200-313)

Avaya CallPilot® Installer Roadmap (NN44200-314)

#### Server Installation Guides

Avaya CallPilot® 201i Server Hardware Installation Guide (NN44200-301)

Avaya CallPilot® 202i Server Hardware Installation Guide (NN44200-317)

Avaya CallPilot® 202i Installer Roadmap (NN44200-319)

Avaya CallPilot® 703t Server Hardware Installation Guide (NN44200-304)

Avaya CallPilot® 1002rp Server Hardware Installation Guide (NN44200-300)

Avaya CallPilot® 1002rp System Evaluation (NN44200-318)

Avaya CallPilot® 1005r Server Hardware Installation Guide (NN44200-308)

Avaya CallPilot® 1005r System Evaluation (NN44200-316)

Avaya CallPilot® 1006r Server Hardware Installation Guide (NN44200-320)

Avaya CallPilot® 600r Server Hardware Installation Guide (NN44200-307)

Avaya CallPilot® 600r System Evaluation (NN44200-315)

#### Configuration and Testing Guides

Avaya Meridian 1 and Avaya CallPilot® Server Configuration Guide (NN44200-302)

Avaya T1/SMDI and Avaya CallPilot® Server Configuration Guide (NN44200-303)

Avaya Communication Server 1000 System and Avaya CallPilot® Server Configuration Guide (NN44200-312)

#### Unified Messaging Software Installation

Avaya CallPilot® Desktop Messaging and My CallPilot Installation and Administration Guide (NN44200-305)

#### Administration

Avaya CallPilot® Administrator Guide (NN44200-601)

Avaya CallPilot® Software Administration and Maintenance Guide (NN44200-600)

Avaya Meridian Mail to Avaya CallPilot® Migration Utility Guide (NN44200-502)

Avaya CallPilot® Application Builder Guide (NN44200-102)

Avaya CallPilot® Reporter Guide (NN44200-603)

#### Maintenance

Avaya CallPilot® Troubleshooting Reference Guide (NN44200-700)

Avaya CallPilot® Preventative Maintenance Guide (NN44200-505)

#### Server Maintenance and Diagnostics

Avaya CallPilot® 201i Server Maintenance and Diagnostics Guide (NN44200-705)

Avaya CallPilot® 202i Server Maintenance and Diagnostics Guide (NN44200-708)

Avaya CallPilot® 703t Server Maintenance and Diagnostics Guide (NN44200-702)

Avaya CallPilot® 1002rp Server Maintenance and Diagnostics Guide (NN44200-701)

Avaya CallPilot® 1005r Server Maintenance and Diagnostics Guide (NN44200-704)

Avaya CallPilot® 1006r Server Maintenance and Diagnostics Guide (NN44200-709)

Avaya CallPilot® 600r Server Maintenance and Diagnostics Guide (NN44200-703)

Avaya NES Contact Center Manager Communication Server 1000/ Meridian 1 & Voice Processing Guide (297-2183-931)

#### End User Information

##### End User Cards

Avaya CallPilot® Unified Messaging Quick Reference Card (NN44200-111)

Avaya CallPilot® Unified Messaging Wallet Card (NN44200-112)

Avaya CallPilot® A-Style Command Comparison Card (NN44200-113)

Avaya CallPilot® S-Style Command Comparison Card (NN44200-114)

Avaya CallPilot® Menu Interface Quick Reference Card (NN44200-115)

Avaya CallPilot® Alternate Command Interface Quick Reference Card (NN44200-116)

Avaya CallPilot® Multimedia Messaging User Guide (NN44200-106)

Avaya CallPilot® Speech Activated Messaging User Guide (NN44200-107)

Avaya CallPilot® Desktop Messaging User Guide for Microsoft Outlook (NN44200-103)

Avaya CallPilot® Desktop Messaging User Guide for Lotus Notes (NN44200-104)

Avaya CallPilot® Desktop Messaging User Guide for Novell Groupwise (NN44200-105)

Avaya CallPilot® Desktop Messaging User Guide for Internet Clients (NN44200-108)

Avaya CallPilot® Desktop Messaging User Guide for My CallPilot (NN44200-109)

Avaya CallPilot® Voice Forms Transcriber User Guide (NN44200-110)

The Map was created to facilitate navigation through the suite by showing the main task groups and the documents contained in each category. It appears near the beginning of each guide, showing that guide's location within the suite.

---

## **Routine maintenance task checklists (daily, weekly, monthly, semi-annual)**

The following four checklists summarize the routine maintenance tasks in this guide according to their recommended frequency: daily, weekly, monthly, or semi-annually. You can photocopy these checklists and use them in your work area as a reminder to perform each task regularly and to establish a routine.

---

## Daily routine maintenance tasks

Date: \_\_\_\_\_

Task	Check
<a href="#">Monitoring event logs for Critical and Major events</a> on page 24	<input type="checkbox"/>
<a href="#">Checking that all call and multimedia channels are in service and can answer calls</a> on page 27	<input type="checkbox"/>
<a href="#">Monitoring traffic using CallPilot Reporter</a> on page 29	<input type="checkbox"/>
<a href="#">Checking LED/HEX displays for error indications</a> on page 44	<input type="checkbox"/>

---

## Weekly routine maintenance tasks

Date: \_\_\_\_\_

Task	Check
<a href="#">Checking the space available in MMFS volumes</a> on page 32	<input type="checkbox"/>
<a href="#">Performing regular full system backups for disaster recovery</a> on page 34	<input type="checkbox"/>
<a href="#">Maintaining archives of users, prompts, applications, and voice forms</a> on page 35	<input type="checkbox"/>
<a href="#">Verifying that scheduled backups are successful</a> on page 36	<input type="checkbox"/>
<a href="#">Rotating tapes</a> on page 36	<input type="checkbox"/>

Task	Check
<a href="#">Checking the backup network share for adequate space</a> on page 37	<input type="checkbox"/>
<a href="#">Performing quick security checks on the server</a> on page 38	<input type="checkbox"/>
<a href="#">Monitoring available hard disk space</a> on page 41	<input type="checkbox"/>
<a href="#">Checking the status of RAID disk packs</a> on page 47	<input type="checkbox"/>

---

## Monthly routine maintenance tasks

Date: \_\_\_\_\_

Task	Check
<a href="#">Checking for and installing the latest server SUs and any required PEPs</a> on page 30	<input type="checkbox"/>
<a href="#">Checking for and installing the latest switch PEPs, and checking dependency lists</a> on page 31	<input type="checkbox"/>
<a href="#">Removing unused mailboxes</a> on page 33	<input type="checkbox"/>
<a href="#">Ensuring all approved Microsoft Security Updates are installed</a> on page 38	<input type="checkbox"/>
<a href="#">Monitoring the health of your hard disks</a> on page 42	
<a href="#">Checking fans and power supplies for proper operation</a> on page 45	<input type="checkbox"/>
<a href="#">Ensuring RAID audible alarm is enabled on 1002rp and 703t</a> on page 49	<input type="checkbox"/>
<a href="#">Checking the hard drive for media errors using the RAID Windows software</a> on page 50	<input type="checkbox"/>

---

## Semi-annual routine maintenance tasks

Date: \_\_\_\_\_

Task	Check
<a href="#">Keeping antivirus software up to date</a> on page 31	<input type="checkbox"/>
<a href="#">Cleaning fan filters</a> on page 46	<input type="checkbox"/>
<a href="#">Cleaning tape drive heads</a> on page 47	<input type="checkbox"/>
<a href="#">Checking the consistency of RAID drives</a> on page 48	<input type="checkbox"/>

---

## Best practices for your site

Use the following guidelines to develop and maintain best practices for your site. While these are not routine maintenance tasks that you must regularly perform, these guidelines can help you prevent problems and optimize system performance.

---

## Maintain a log book

Maintain a daily log book with recorded maintenance activity. The log book is extremely useful for diagnosing problems. The log book should describe the activity, indicate who performed it, and when it was performed. Include the following activities:

- system operations on the CallPilot server or the telephony switch, such as
  - installations

- upgrades
- PEP installations
- hardware replacement
- administrative updates, such as
  - user additions, deletions, or modifications
  - system parameter changes
- problem investigation

---

## Use only qualified technicians to work with the CallPilot system

Only CallPilot qualified technicians must administer or maintain the CallPilot server. As mentioned in [Maintain a log book](#) on page 15, all activities performed on the CallPilot server should have a name associated with the activity recorded in the log book.

---

## Ensure recovery media is on-site

A current full system backup is essential for system recovery in case an error occurs during an upgrade or if hardware fails. A full system backup applies to all systems, RAID-equipped or not. For details about performing a backup, see the Administrator Guide (NN44200-601) or the CallPilot Manager online Help.

Ensure recovery media for your current system setup is on-site. Include the following items:

- Most recent backup (tapes or access to remote disk)
- CallPilot Image CDs or DVD
- CallPilot Language Prompts CD
- CallPilot Applications CD
- PEP CD

Depending on your system setup, you need the following items:

- My CallPilot Software CD
- CallPilot Desktop Messaging CD
- Windows Operating System CD (for stand-alone Web server configuration)
- Antivirus software

---

## Ensure recovery hardware is on-site

Ensure that any required hardware is on-site. This hardware includes the following items:

- Replacement hard drive
- Replacement multimedia cards
- Replacement RAID controller (if your system has RAID)
- Tape drive
- Optionally: Replacement CD-ROM drive or DVD-ROM drive

Proper maintenance and operation of CallPilot requires that adequate spares are available within time frames that are conducive to minimizing downtime at a customer location if a failure occurs. Information regarding proper spares planning, critical spares, field replaceable units, as well as recommended field service kits are available within Product Bulletin P-2005-0243-Global, CallPilot Spares Planning.

---

## Ensure no unauthorized third-party software is installed on the server

As described in CallPilot documentation and within Product Bulletin 99067, CallPilot Unauthorized Hardware and Software, do not install third-party software on the CallPilot server unless specifically authorized in a CallPilot product bulletin. Severe performance problems can result.

Unauthorized software includes the following:

- CallPilot client software:
  - Application Builder
  - Desktop Messaging clients
- Unauthorized third-party software:
  - Windows Server backup utilities
  - Monitoring and diagnostic utilities
  - Antivirus applications not identified within the authorized list
  - FTP software
  - Spyware detection software
  - Instant Messaging (IM) software

- Browser add-ons or plug-ins
- Media player software
- security hardening scripts, tools and utilities
- software firewalls

Authorized third-party software includes the following:

- Certain versions of antivirus software  
  
See the Avaya product bulletin titled CallPilot Support for Anti-Virus Applications (P-2007-0101-Global) for updated information about the antivirus applications tested and approved for installation on CallPilot.
- Software Avaya includes in the base product, for example, pcAnywhere (for remote support) and Acrobat Reader.
- EMC AutoStart software (for High Availability systems only)

---

## **Do not surf the Internet on the CallPilot server**

Use the Internet only when necessary on the CallPilot server, for example, to download Microsoft patches or antivirus software updates. Do not install browser add-ons or plug-ins; they can use up significant amounts of memory and degrade server performance. Browsing the Internet can also pose security risks, so when you must use the Internet, maintain high security settings in your browser and visit only known Web sites. Close the browser when you are finished using it.

---

## **Log off the local Windows console when not in use**

This terminates interactive programs and frees up memory. Note that most administrative actions can be performed using a browser on a client PC. Under normal circumstances, it is not necessary to use the local Windows console of a CallPilot server.

---

## **Do not apply customer-specific security hardening scripts to the CallPilot server**

CallPilot systems are already hardened for tight security. Applying customer-specific hardening scripts can damage the system and can result in your server needing to be reimaged.

---

## **Safeguard your CallPilot passwords and change them periodically**

Store an up-to-date list of administrative CallPilot passwords in a safe place with limited access; do not display them. Change them periodically, particularly if there is staff turnover in the server administration group or if you suspect suspicious activity.

---

## **Ensure remote access is operational**

You must have a modem to support remote dial-up access to the CallPilot server. With a modem, Avaya Technical Support can connect to your CallPilot server to troubleshoot problems. Avaya connects to your server only when you request technical assistance.

Ensure that the modem is operational and that a Remote Access Service (RAS) connection can be established when required. For improved security, the modem can be disconnected from the telephone line if there is no current need for remote support. See your specific Server Hardware Installation Guide.

---

## **Ensure proper power and grounding**

All CallPilot server installations must follow proper power and grounding procedures, specifically, adhering to the single-point ground reference requirement. For detailed information about proper power and grounding, see your specific Server Hardware Installation Guide and the Planning and Engineering Guide (NN44200-200).

Failure to follow these guidelines makes the Meridian 1, Communication Server 1000, or CallPilot susceptible to damage from electrical transients resulting from lighting and other powerground disturbances.

Ensure that a single-point ground reference is available for all power outlets that serve the CallPilot server and its peripherals. Before the CallPilot server installation, a qualified electrician must implement the single-point ground reference requirement between the power outlets of the CallPilot server and the power outlets of the switch.

The single-point ground reference includes all powered devices that attach directly to the switch and its ancillary equipment. For a typical CallPilot installation, the following components are included:

- Switch
- CallPilot server
- Uninterruptible Power Supply (UPS) (if installed)
- Modem (non-USB modem)
- ELAN and CLAN Ethernet switches or hubs
- Administration and Maintenance PC (and associated printer)
- Contact Center Manager Server (if installed)

Avaya strongly recommends that you equip tower and rackmount installations with a UPS. Use of a UPS that supports the server and the ELAN and CLAN Ethernet switches or hubs ensures the following conditions:

- no outages from power disruptions
- reduces potential for data corruption caused by power disruptions

---

## Ensuring all external cables are secured to their connectors

 **Important:**

The system must be powered off when checking external cables.

Each time you power the system off, check all external cables and connectors by inspecting and gently pulling the cable to ensure it is firmly connected. You must check connectors that can be manually screwed in place and, if necessary, tighten the connectors to ensure they are secure. It is good practice to secure the external cables with the provided screws. Check that all RJ-45 connectors are firmly crimped to the sheath of the cable. Where applicable, ensure that SCSI terminators are in place and firmly tightened. It is also a good practice to ensure that all external cables are properly labeled.

---

## Ensure systems have a proper operating system certificate attached

Each system must have the proper operating system (OS) certificate attached. Ensure that the Microsoft Windows 2003 Certificate of Authenticity (COA) is attached to the system. If you are

upgrading from a previous CallPilot release on an older operating system, the COA label is included in the upgrade kit; remember to attach it to the upgraded system.

---

## Ensure the system is properly labeled

Ensure all components, cables, and ports are properly labeled. A properly labeled system helps you troubleshoot your system and identify parts of the CallPilot system. If you have a rackmount server, ensure the CallPilot server is labeled to distinguish it from other servers in the rack.

---

## Follow recommended handling procedures when removing power from a 200 series server from the PBX shelf

To minimize data loss or damage to the drive media, when removing power from the 201i or 202i IPE server, ensure the system avoids excessive vibration until the hard drive heads have parked. Use the following recommended handling procedure.

### **Removing power from a 201i with 3.5 inch desktop hard drives and Windows NT**

1. To power off the server, press Ctrl + Alt + Delete, and then click Shutdown.  
Windows has shut down when the screen fades to black and the word DOWN appears on the green HEX display.
2. Unseat the card lock latches and remove power by gently unseating the server from the backplane.
3. Remove the server from the card shelf and handle normally following ESD guidelines
4. Allow the server to remain still for approximately 15 seconds. This allows the drive heads to park to a safe zone.
5. Remove the server from the card shelf and handle normally following ESD guidelines.

### **Removing power from a 201i with 2.5 inch mobile and 3.5 inch desktop hard drives and Windows 2003**

1. To power off the server, press Ctrl + Alt + Delete, and then click Shutdown.  
Windows has shut down when the screen fades to black and the word DOWN appears on the green HEX display.
2. Remove the server from the card shelf and handle normally following ESD guidelines.

### **Removing power from a 202i with 2.5 inch mobile hard drives and Windows 2003**

1. To power off the server, press Ctrl + Alt + Delete, and then click Shutdown.  
Windows has shut down when the screen fades to black and the word DOWN appears on the green HEX display.
2. Unseat the card lock latches and remove power by gently unseating the server from the backplane.
3. Remove the server from the card shelf and handle normally following ESD guidelines
4. Allow the server to remain still for approximately 15 seconds. This allows the drive heads to park to a safe zone.
5. Remove the server from the card shelf and handle normally following ESD guidelines.

# Chapter 4: Routine maintenance tasks: software and database maintenance

This chapter contains the following topics:

- [Monitoring server performance and traffic](#) on page 24
- [Monitoring event logs for Critical and Major events](#) on page 24
- [Archiving Flight Recorder information](#) on page 25
- [Viewing Flight Recorder archive statistics](#) on page 26
- [Downloading Flight Recorder archives](#) on page 26
- [Deleting Flight Recorder archives](#) on page 26
- [Tip: Setting up an alarm mailbox so you are notified of alarms](#) on page 27
- [Checking that all call and multimedia channels are in service and can answer calls](#) on page 27
- [Monitoring traffic using CallPilot Reporter](#) on page 29
- [Keeping your software up-to-date](#) on page 30
- [Maintaining adequate storage space](#) on page 32
- [Performing regular full system backups for disaster recovery](#) on page 34
- [Maintaining archives of users, prompts, applications, and voice forms](#) on page 35
- [Verifying that scheduled backups are successful](#) on page 36
- [Rotating tapes](#) on page 36
- [Checking the backup network share for adequate space](#) on page 37
- [Keeping the system secure](#) on page 37
- [Ensuring all approved Microsoft Security Updates are installed](#) on page 38
- [Performing quick security checks on the server](#) on page 38

 **Note:**

The information in this section contains references to software and bulletins that are posted on various Avaya Web sites. Some of these Web sites require registration or are restricted to Avaya channel partners. If you cannot get access to a document you want, contact your Avaya channel partner.

---

## Monitoring server performance and traffic

Avaya CallPilot® provides monitoring tools that you can use to identify potential or existing problems with the performance of your server. These tools include the Alarm Monitor, Channel Monitor, Multimedia Monitor, Performance Monitor, and the reports in Avaya CallPilot Reporter. The following sections describe key preventative maintenance tasks that you can perform using these tools.

---

## Monitoring event logs for Critical and Major events

Frequency: Daily

To ensure you are aware of service-affecting events so that you can take appropriate action, check daily your Avaya CallPilot event logs. This is one of the most important preventative maintenance tasks. CallPilot is designed so that if there is a system problem, in most cases, there is a corresponding alarm. Investigate any unusual alarms or events, changes in alarm patterns, or inordinate alarm volumes.

Take into account that Windows makes auto-backup of event logs when they reach maximum configured size. Archived logs are saved into the same directory which contains evt-files of the current logs. This directory is C:\WINDOWS\system32\config by default. Archive file names follow 'Archive-<Log>-<DateTime> .evt template. <Log> can be Application, Security or System. <DateTime> is a timestamp generated when the log was archived. If you would like to check the events stored in the archived log file, you can open the file in Windows Event Viewer.

You can view Event Logs in three places: the CallPilot Event Browser, the CallPilot Alarm Monitor, and the Windows Event Viewer in the operating system. Consider using the Alarm Monitor to focus on problems that require correction. It shows only Minor, Major, and Critical events, and ignores Information events. In addition, when an event occurs repeatedly, it is reported only one time in the Alarm Monitor to avoid cluttering the Alarm Monitor display.

### To check for Critical and Major events in Alarm Monitor

1. In CallPilot Manager, click System > Alarm Monitor.
2. Review the alarms that occurred since the last time you checked.  
Pay particular attention to Critical or Major events, which indicate that urgent corrective action is required.
3. To view additional information about an event, click the event number to display a Help topic.

4. Take the required steps to resolve any problems.
5. After you address each event and complete your check, clear the events from the Alarm Monitor.

For more information about monitoring events using Event Browser, Alarm Monitor, or the Windows Event Viewer, see the following documentation:

- Administrator Guide (NN44200-601)
- CallPilot Manager online Help

---

## Archiving Flight Recorder information

Flight Recorder (FR) continuously captures key performance counters, traces, logs, and events on your system. As an administrator, you can archive this information in order to make it available for diagnostic purposes.

Flight Recorder log files for all platforms (except 703t) are stored on the CallPilot server in the C:\CallPilot\Flight Recorder directory. Log files for the 703t server are stored in the D:Nortel\Flight Recorder. Flight Recorder archives are stored in the C:\inetpub\wwwroot\cpmgr\Upload directory.

### Important:

There is a threshold for the amount of disk space that can be consumed by archives. If the amount of free space on the drive where logs are stored drops below 10%, Flight Recorder blocks any further creation of archives and logs. In this situation, archive creation and logging does not resume until the amount of free space rises above 12%. Increasing the amount of free space can be achieved by deleting archives. For information on how to delete archives, refer to [Deleting Flight Recorder archives](#) on page 26.

- 
1. Log on to CallPilot Manager.
  2. Click **Maintenance > Flight Recorder**.
  3. Select **Archive Manager** from the **Select a task** drop-down list.
  4. Select the module(s) for which you want to archive the data.
  5. Click **Archive**.  
The Archiving Progress screen will display. To abort the archive click the **Cancel** button.

### Note:

The duration of the archiving process is dependent upon the amount of data being archived and the current system load. As a result, archiving may take a significant amount of time or even be cancelled altogether due to time out. In case of any

problems, additional information can be found in the Flight Recorder log file (C:\CallPilot\flr.log) and in the Windows Application Event log.

6. When the archive is complete, click **Close**.
- 

---

## Viewing Flight Recorder archive statistics

The Download Manager displays all archives that have been created, the amount of disk space being used by the archives, and the maximum allowed disk space that archives can consume.

- 
1. Log on to CallPilot Manager.
  2. Click **Maintenance > Flight Recorder**.
  3. Select **Download Manager** from the **Select a task** drop-down list.  
The Download Manager window displays archives and associated disk information.
- 

---

## Downloading Flight Recorder archives

As an administrator, you can download archives captured by Flight Recorder at any time. If a server outage occurs, archives can be sent to support personnel and product design teams to determine what caused the outage.

- 
1. Log on to CallPilot Manager.
  2. Click **Maintenance > Flight Recorder**.
  3. Select **Download Manager** from the **Select a task** drop-down list.
  4. Click the link to the archive you want to download and save it to a specific location on your PC.
- 

---

## Deleting Flight Recorder archives

As an administrator, you can delete aging archives that are unnecessarily consuming disk space.

- 
1. Log on to CallPilot Manager.
  2. Click **Maintenance > Flight Recorder**.
  3. Select **Download Manager** from the **Select a task** drop-down list.
  4. Select the archive(s) you want to delete and click **Delete Selected**.
- 

---

## Tip: Setting up an alarm mailbox so you are notified of alarms

You can configure CallPilot to send you a voice message when an alarm is generated. You can specify the severity of alarms for which you want this notification. If you want immediate notification of new alarms, you can then set up remote notification to forward the notification message to another telephone or a pager.

### To set up an alarm mailbox

1. In CallPilot Manager, click Messaging > Messaging Management.
2. Scroll to the Special Purpose Mailboxes settings.
3. In the Alarm Mailbox Number box, type the number of the mailbox to which you want alarm notifications sent.
4. In the Severity to Trigger list, specify which alarms are to generate a message.
5. Click Save.
6. You can set up remote notification for the alarm mailbox, if required. For more information, see the online Help in CallPilot Manager.

 **Note:**

If there are certain events for which you no longer want to receive notification, you can decrease their severity level (for example from Major to Minor) in the Event Browser. For more information on customizing events, see the online Help in CallPilot Manager.

---

## Checking that all call and multimedia channels are in service and can answer calls

Frequency: Daily

Check the state of call and multimedia channels in CallPilot Manager to ensure that the server is not experiencing trouble processing incoming calls, and to ensure no channels are off duty.

Call channels are the connections between the server and the switch that carry the call signals to CallPilot. Multimedia channels are the DSP ports that process the calls.

### To check proper operation of call channels

1. In CallPilot Manager, click Maintenance > Channel Monitor.
2. In the Channel Status grid, view the status of the call channels to ensure they are problem free. Properly operating call channels should show one of the following statuses:

	The channel is currently processing call data or has completed call processing in the last 30 seconds.
	The channel is working but not currently transporting call data to the server.

Certain statuses can flag a problem, as shown in the following examples:

	The channel has been stopped.
	The channel has been taken out of service at the switch.
	The channel has been disabled as a result of a failed diagnostic test or a hardware failure.
	The hardware required for channels to operate is not installed or is not operating properly.

For information about other call channel statuses and what they mean, click the Help button in Channel Monitor, and then click the status link. You can also view information about channels using the CallPilot System Monitor utility.

3. If issues exist with call channels, take action to resolve them.

### To check proper operation of multimedia channels

1. In CallPilot Manager, click Maintenance > Multimedia Monitor.
2. In the Channel Status grid, view the status of the multimedia channels to ensure they are problem free. Properly operating multimedia channels should show one of the following statuses:

	The channel is currently processing call data or has completed call processing in the last 30 seconds.
	The channel is working but not currently transporting call data to the server.

Certain statuses can flag a problem, as shown in the following examples:

	The channel has been stopped.
	The channel has been taken out of service at the switch.
	The channel has been disabled as a result of a failed diagnostic test or a hardware failure.
	The hardware required for channels to operate is not installed or is not operating properly.

For information about other multimedia channel statuses and what they mean, click the Help button in Multimedia Monitor, and then click the status link. You can also view information about channels using the CallPilot System Monitor utility.

3. If there are issues with multimedia channels, take action to resolve them.

For more information about Channel Monitor and Multimedia Monitor, see the Administrator Guide (NN44200-601).

For more information about troubleshooting your CallPilot system, see the following documentation:

- Troubleshooting Reference Guide (NN44200-700)
- Server Maintenance and Diagnostics (for your server type)

---

## Monitoring traffic using CallPilot Reporter

Frequency: Daily (or as applicable to each report type)

You can use CallPilot Reporter to generate a multitude of reports that contain valuable information about your CallPilot system. Ensure you are aware of the available reports and that you are regularly generating and analyzing reports (daily, weekly, and monthly, as applicable to each type of report). This way, you can establish a pattern of normal behavior or baseline for your system. Use this baseline to differentiate between normal system activities and unusual or suspicious activities. When you establish a baseline, you can use reports to identify potential problems. Here are some examples:

- Channel Usage Reports from the last three months show that each of your channels processes an average of 50 calls per hour. If one channel suddenly drops to only three or four calls per hour, this can indicate a problem with your system hardware or configuration.
- If the Service Quality Summary Report indicates that callers are experiencing a lengthy wait time before they access a channel, sufficient channels may not be available to handle the volume of traffic. You might need to increase the number of channels on the system if the volume of traffic is higher than originally anticipated.

You can set up a schedule for your reports so they are generated automatically at specified times. For more information about the available reports and how they can help you identify potential problems, see the Reporter Guide (NN44200-603).

---

## Keeping your software up-to-date

To ensure the software on your CallPilot server and switch remains up-to-date, perform the preventative maintenance tasks described in this section.

---

## Checking for and installing the latest server SUs and any required PEPs

Frequency: Monthly, or when new SUs and PEPs become available

Avaya periodically releases new Service Updates (SUs) and Product Enhancement Packages (PEPs) for the CallPilot server. These files contain changes to the CallPilot software, for example, fixes for known issues or enhancements to existing features. All SUs and PEPs for a CallPilot release are available for download from the ESPL Web site at [www.avaya.com/support](http://www.avaya.com/support).

You must keep your server up-to-date by installing the latest SUs and any required PEPs as they become available. You can register to receive automatic notification of new Service Updates and PEPs at [www.avaya.com/support](http://www.avaya.com/support).

 **Note:**

On the Technical Support Web site at [www.avaya.com/support](http://www.avaya.com/support), you can use the My Email Alerts feature to receive an e-mail when software updates become available.

### To check for and install the latest server SUs and any required PEPs

1. Access the ESPL Web site at the following URL:  
[www.avaya.com/support](http://www.avaya.com/support)
2. Navigate to the Multimedia PEP Tools section, and then search for CallPilot SUs and PEPs for your platform and release.
3. If there are any SUs or required PEPs listed that are not currently on your CallPilot server, install them.

 **Note:**

To check which SUs and PEPs are currently installed, on the CallPilot server, click Start > Programs > CallPilot > System Utilities > PEP Maintenance Utility.

For more information and detailed procedures, see the following documentation:

- For specific SU or PEP installation instructions, see the readme files that are provided with the SU or PEP. In many cases, you must install and uninstall SUs and PEPs in a specific order. The readme files provide these instructions.
- For general SU or PEP installation instructions, see Software Administration and Maintenance (NN44200-600).

---

## Checking for and installing the latest switch PEPs, and checking dependency lists

Frequency: Monthly, or when new switch PEPs become available

Avaya periodically releases new PEPs for the switch that your CallPilot server connects to. These files contain changes to the switch software, for example, fixes for known issues or enhancements to existing features. Like server PEPs, switch PEPs are also available for download at [www.avaya.com/support](http://www.avaya.com/support).

To keep your switch up-to-date, install the latest PEPs as they become available and check the dependency lists. Avaya recommends that you check monthly the ESPL Web site to ensure you are aware of any recent additions.

---

## Keeping antivirus software up to date

Frequency: Check for bulletin updates every six months or before updating antivirus applications

Use of an antivirus application on the CallPilot server helps to ensure it remains virus-free. Before you install or update antivirus software, download the latest version of the Avaya Product Bulletin. CallPilot Support for Anti-Virus Applications, and follow the instructions and guidelines.

This detailed product bulletin includes the following information:

- a list of supported antivirus applications for each CallPilot release
- a list of best practices for keeping the server virus-free
- specific installation, configuration, and operation requirements for each supported antivirus application

Avaya periodically reissues this product bulletin to add support for new versions of antivirus applications, so ensure you have the latest version before you make related changes. Each

antivirus application has specific configuration and operation requirements; improper configuration can result in CallPilot service degradation or outages.

This product bulletin is available on the <http://www.avaya.com> Web site, in the Partner Information Center (PIC).

---

## Maintaining adequate storage space

Perform the following preventative maintenance tasks to ensure the CallPilot server has adequate storage space.

---

## Checking the space available in MMFS volumes

Frequency: Weekly

Using CallPilot Reporter, run the Multimedia File System Usage Monitor Report each week to determine whether the system has sufficient space to handle the current messaging and multimedia applications. If a Multimedia File System (MMFS) volume becomes full, users with mailboxes on that volume cannot create or receive any new messages. For each MMFS volume, usage should remain below 90 percent.

The CallPilot server generates the following events when the a volume becomes too full:

Event code	Severity	Description
40241	Major	A multimedia disk volume is 90% full.
40241	Critical	A multimedia disk volume is 95% full.

If any volume is above 90 percent, then you must free up space on that volume. Strategies to clear space include the following:

- If only one volume is full, you can move users' mailboxes from the full volume to another volume.
- If all volumes are nearing capacity, you can try:
  - forcing the system to delete reviewed messages after an appropriate retention period, or shortening the current period (use the mailbox class setting Delete Read Voice Messages)
  - looking at usage reports to determine which users use a lot of space, and talk to them about it
  - deleting any unnecessary Application Builder applications

- removing unused mailboxes (see [Removing unused mailboxes](#) on page 33)

If the system is chronically low on space, consider moving to a larger platform, particularly if you must add new users to the system.

Ensure that the nightly MMFS volume audit is completing successfully. This recovers space that may have been lost due to error conditions, program crashes, or system restarts. The MMFS volume audits occur on each MMFS volume every morning at 3 a.m. Also, ensure that the nightly Garbage Daemon audit is completing successfully. The Garbage Daemon audit occurs every morning at 3:30 a.m. It deletes read messages after the retention period has expired.

Check for the following events related to these audits (40232 and 55041 can indicate a problem):

Event code	Time	Severity	Description
40236	3 a.m.	Info	An audit of a multimedia volume has begun.
40233	after 3 a.m.	Info	An audit of a multimedia volume completed successfully. The number of lost disk blocks recovered is given.
40232	after 3 a.m.	Major	An audit of a multimedia volume failed. Lost disk blocks were not recovered.
55039	3:30 a.m.	Info	Garbage Daemon audit started.
55040	after 3:30 a.m.	Info	Garbage Daemon audit completed.
55041	3:30 a.m.	Minor	The Garbage Daemon audit failed to run.

For a complete list of strategies for reducing mailbox sizes, see the Administrator Guide (NN44200-601).

For more information about running and interpreting the Multimedia File System Usage Monitor Report, see the Reporter Guide (NN44200-603).

---

## Removing unused mailboxes

Frequency: Monthly

Using CallPilot Reporter, run the Inactive User Report each month to identify mailboxes that might no longer be in use. This report identifies users who no longer log into their mailbox or read messages. This can indicate a user who is on leave or on vacation, but it can also indicate a mailbox that is no longer in use and you should remove it. Mailboxes that exist in the system but are not in use can use valuable MMFS space as broadcast messages build up. Also,

mailboxes that belong to former employees that are on the CallPilot system can cause a potential security concern.

 **Note:**

If your site does not have CallPilot Reporter, as an alternative, you can use the Advanced User Search function in CallPilot Manager to find mailboxes that may no longer be in use. Use the search criterion Time of Last Login to search for stale mailboxes.

For information about running and interpreting the Inactive User Report, see the Reporter Guide (NN44200-603).

For information about deleting mailboxes, see the following documentation:

- Administrator Guide (NN44200-601)
- CallPilot Manager online Help

---

## Maintaining up-to-date backups

To protect your site against data loss, maintain up-to-date backups. Review the chapter about backing up and restoring CallPilot information in the Administrator Guide (NN44200-601); the chapter provides detailed information about backup types, ways to ensure backup safety, and information about scheduling backups. The following sections summarize key aspects of preventative maintenance through backups.

---

## Performing regular full system backups for disaster recovery

Frequency: Weekly

Ensure you have a full system backup scheduled at regular intervals, even on systems equipped with RAID. A full system backup backs up all critical data, including messages and configuration information, on all drives (neither the operating system nor the CallPilot software are backed up). A full system backup is critical to prevent data loss if a system failure occurs, such as a disk drive failure or data corruption. Many recovery scenarios require you to restore a full system backup, so it is critical to have an up-to-date backup on hand. You should also perform a full system backup before upgrading or installing new software.

You can schedule backups to run online while the system is still in service; however, Avaya recommends that you schedule backups for off-peak hours.

For more information about how and when to schedule full system backups, see the following documentation:

- Administrator Guide (NN44200-601)
- CallPilot Manager online Help

---

## Maintaining archives of users, prompts, applications, and voice forms

Frequency: Weekly, or whenever you make changes to related data

Archives are copies of multimedia files from CallPilot. It is important that you back up this data regularly, or whenever you make changes.

The following table summarizes the archive types and shows the recommended backup frequency.

Type of archive	Information in archive	Recommended backup frequency
user archive	messages, greetings, personal verifications, plus mailbox configuration information	frequently at regular intervals   <b>Note:</b> Choose a frequency that makes sense for your site. For example, consider backing up certain high-profile mailboxes daily due to their importance; for other mailboxes, a weekly or monthly backup may suffice. If you have recently added a lot of mailboxes, it is a good idea to create an archive right away.
prompt archive	all custom prompts recorded in a single language	periodically and whenever you add or update applications
AppBuilder archive	custom applications created using Application Builder	whenever you add or update voice prompts
voice form archive	voice form configuration data and prompts	whenever you add or update voice forms

For more information about how to schedule archives, see the following documentation:

- Administrator Guide (NN44200-601)
- CallPilot Manager online Help

---

## Verifying that scheduled backups are successful

Frequency: Weekly, or after each backup you schedule

In addition to scheduling backups, you must regularly check backup logs to ensure they are successful and, more importantly, to be aware of failed backups. For example, if you schedule a backup to a network drive and that drive runs out of space, the scheduled backup will fail. To avoid such problems going unnoticed, use CallPilot Manager to check the backup history for each backup. To troubleshoot, you can view backup logs (Summary Logs and Detail Logs) for both full system backups and archives.

### To check that backups are successful

1. Open CallPilot Manager, and then click System > Backup/Restore.
2. Click View Backup History.
3. You can select from Select the archive types to display in the list.
4. Check the Status column, and look for Operation Completed, which indicates the backup was successful. If you see Operation Failed or Operation Partially Completed, you must check the backup logs to troubleshoot the failure.
5. To view backup logs, click either Summary Log or Detailed Log.
6. Resolve any issues with failed backups, and then run the backup again. Never restore a partially completed backup.

 **Note:**

To avoid using space unnecessarily, delete old backup log files when you no longer need them. The logs are stored at D:\nortel\data\backup\BackupLogs.

---

## Rotating tapes

Frequency: Weekly

If you back up data to a tape drive, ensure you set up a tape rotation schedule to use a different tape each week (or as required, depending on your backup schedule). Tape media that is used frequently eventually wears out and ceases to protect data properly. Ensure that you use multiple tapes in a rotation scheme to prevent potentially overwriting good data with bad when you perform tape backup or archives. Rotating several tapes extends individual tape life and enhances data resiliency.

Example of a three-tape rotation is as follows:

- Week 1 use tape 1
- Week 2 use tape 2
- Week 3 use tape 3
- Week 4 repeats cycle with tape 1

---

## Checking the backup network share for adequate space

Frequency: Weekly

If you back up data to a shared directory on a remote computer, you must ensure that sufficient space is available for backup files created during your scheduled backups. Each scheduled backup creates a new backup file. If unattended, the drive can eventually become full and your scheduled backups will no longer complete successfully.

To avoid this situation, determine how many backup files you can afford to store in the network share at one time. Regularly move old backup files from the network share to another storage medium, such as a DVD, or delete them. Alternatively, if your site has a network-wide backup application, consider configuring it to pick up the CallPilot backups from the network share. The size of each subsequent backup file can grow over time, so monitor the network share each week to ensure adequate space is still available.

### To check the backup network share for adequate space

1. Log on to the remote computer that contains the shared directory you use for backups, and then navigate to the shared directory.
2. Check the sizes of your most recent backups and note the total size.
3. Check the available space on the drive that contains the shared directory.

If the available space is inadequate, consider clearing other files from the drive to free up space, reducing the number of backup files you retain in the shared directory, or moving the network share to a computer with more available space.

---

## Keeping the system secure

Help protect the CallPilot system from security vulnerabilities by performing the preventative maintenance tasks described in the following sections.

---

## Ensuring all approved Microsoft Security Updates are installed

Frequency: Monthly, or as required

Monthly, or as required, check the [www.avaya.com/support](http://www.avaya.com/support) Web site for the latest approved Microsoft Security Updates and apply them as needed for operating-system-specific fixes. When Microsoft issues a new Security Update, Avaya evaluates whether it applies to CallPilot, its threat-severity, and its impact on CallPilot operation and stability. After successful testing on software releases, Avaya approves the security update for direct download from Microsoft and installation on a CallPilot server. Mid-month (normally the Friday following the second Tuesday), Avaya updates Product Bulletin P-2007-0010, CallPilot Server Security Update, with the latest approved Microsoft Security Updates.

Failure to apply the updates can leave the system susceptible to one or more vulnerability, which can cause a system outage or service degradation, if exploited.

### **Important:**

Except in emergency situations, do not install any Microsoft Security Updates that Avaya has not approved. Never install any Microsoft Service Packs unless Avaya has approved them for your CallPilot release.

### **Note:**

Periodically, Avaya makes all applicable Microsoft Security Updates available in a CallPilot Server Security Update PEP (for current CallPilot releases only). These PEPs provide a convenient installation package that you can use to apply to CallPilot servers during scheduled maintenance windows, typically at the same time you apply a CallPilot SU. These CallPilot Server Security Update PEPs can contain Microsoft security updates that you already manually applied to the server in response to a published bulletin or alert; if so, you need not remove the manually applied Security Updates before you install the CallPilot Server Security Update PEP. The CallPilot Server Security Update PEP overwrites any existing files during installation.

---

## Performing quick security checks on the server

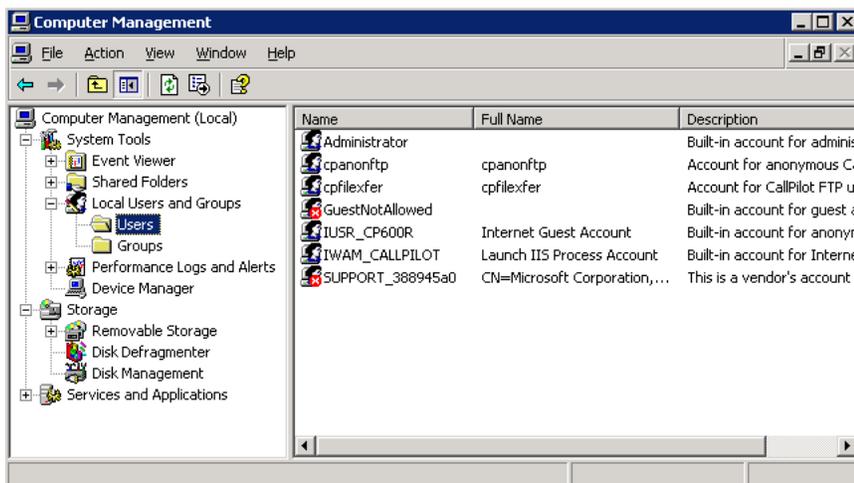
Frequency: Weekly

The following are quick checks you can perform on the server to keep security tight.

## To check for unauthorized Windows users or shared folders

1. On the CallPilot server, from the Windows Start menu, click Programs > Administrative Tools > Computer Management.
2. In the left pane, expand System Tools, and then expand Local Users and Groups.
3. Click Users.

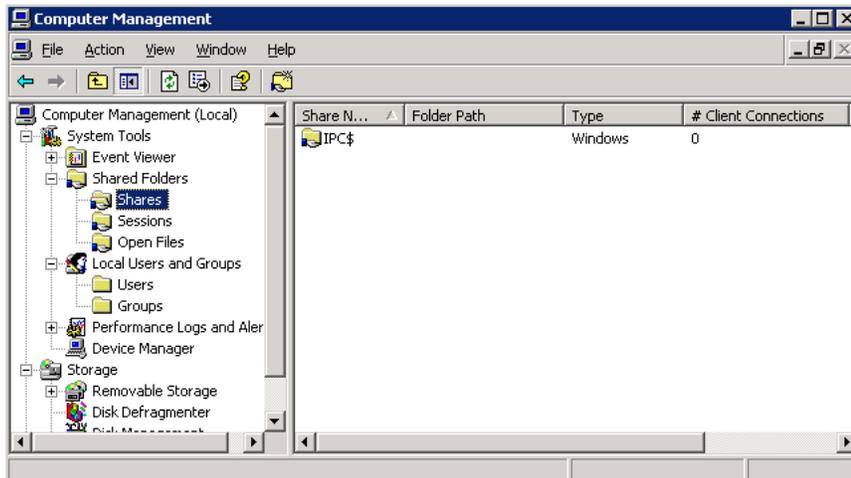
In the right pane, the list of Windows users for the server appears. The following illustration shows the required Windows users. Note that the names of the IUSR\_ and IWAM\_ users can appear differently than shown here; the specific computer name of your server appears after the underscore.



If My CallPilot is installed, an additional user account, MyCallPilotAccount, appears in the list.

4. If there are any additional suspicious users, disable or remove them.
5. To check for unauthorized shared folders, in the left pane, expand Shared Folders.
6. Click Shares.

In the right pane, the list of shared folders users for the server appears. The following illustration shows the shared folder IPC\$, which you should expect to see. On some systems, an additional share named Z\$ can also appear.



7. If there are any additional suspicious shares, disable or remove them.

### To check for unauthorized software

1. On the CallPilot server, from the Windows Start menu, click Settings > Control Panel.
2. Double-click Add or Remove Programs.
3. Check the list of installed programs. Remove any unauthorized software. For a list of authorized software, see the best practices task [Ensure no unauthorized third-party software is installed on the server](#) on page 17.

### To check that antivirus definitions are kept up-to-date

How you perform this check depends on the antivirus software you are using, so the procedure below provides only high-level steps.

1. Open the antivirus console for the software you are using.
2. Check the date of the virus definitions. Avaya recommends that they should be no older than one week.
3. Check to ensure that file access protection is enabled.  
This option is named differently depending on your antivirus software. Examples are real-time checking, on-access scanning, or filesystem autoprotect.
4. If a scheduled virus scan is set up, check that it has been running as expected.

 **Note:**

Ensure you schedule virus scans during off hours.

5. Check that no viruses have been found (look in Quarantine).

# Chapter 5: Routine maintenance tasks: hardware maintenance

This chapter contains the following topics:

- [General maintenance tasks](#) on page 41
- [Maintaining server parts and cabling connections](#) on page 45
- [Maintaining RAID drives](#) on page 47

---

## General maintenance tasks

Ensure your server functions properly by following these general maintenance tasks.

---

## Monitoring available hard disk space

Frequency: Weekly

The amount of available disk space affects the performance of your Avaya CallPilot® system. In some circumstances, the server can stop functioning. Avaya systems provide adequate space to meet your data storage and system operation requirements; however, you must occasionally monitor disk space.

Use Windows Disk Management to view available hard disk space and partitioning information, such as disk partition capacity, free space, and percent free space.

For more information, see the Administrator Guide (NN44200-601).

The following alarms can indicate that disk space on your C drive is too low:

Event code	Severity	Description
40102	Major	Event from Event Scheduler[nbschsrv.dll] : Event Scheduler Debut name=UpdateFlagsInDb, msg=Error: rc=40135 <= CLDAPClient::Update rc=60657. RDN=jobid=12 This event indicates that an internal error occurred when accessing the database.

Event code	Severity	Description
		Note: In the Event Browser description (example shown above), look for rc=60657, which means Logical drive is almost full, some operation might be restricted. Check the available space on C drive.
35903	Major	Event from AOS[] : GetLogRecords failed in Fault This event occurs when you try to display a large number of events in the Avaya CallPilot Event Browser. This operation requires space on the C drive; the event occurs if there is not enough space on the C drive.

## Monitoring the health of your hard disks

Frequency: Monthly

To minimize the possibility of a hard drive failure, there are several proactive checks you can perform each month. These checks are particularly useful for servers that do not have RAID drives (the 201i, 202i, and 600r models), because disaster recovery on these servers can be a prolonged procedure.

The first step is to monitor for certain server events in the System Log of the Windows Event Viewer. These events can indicate that a disk failure is imminent.

### To check the Windows Event Viewer for events related to disk errors

1. On the CallPilot server, open the Windows Event Viewer by clicking Start > Programs > Administrative Tools > Event Viewer.
2. In the left pane, click System.
3. Look for the events listed in the following table.

 **Note:**

To sort the list by event numbers, click the Event column header.

Events	Description
11	The driver detected a controller error on \Device\Scsi\symc8xx1.
9	The device, \Device\ScsiPort0, did not respond within the timeout period. or The device, \Device\Scsi\symc8xx1, did not respond within the timeout period.
7	The device, \Device\Harddisk0\Partition2, has a bad block.

Events	Description
5	A parity error was detected on \Device\Scsi\symc8xx1.

- If you see any of these events, continue to the following procedure to check for errors on the disks. The events in the previous table usually indicate that disk failure is imminent.

In the next procedure, you must run the Windows disk check utility to check a specified disk on the server and display the results. First, run the disk check utility without any of the repair options selected. Then, if the utility detects errors, Avaya recommends that you obtain a new drive as soon as possible. Next, with the new drive on hand as a spare, attempt to run the disk check utility again and select the options to fix errors on the disk. Occasionally, correcting errors on an older disk can lead to total disk failure.

### **Important:**

The following procedure requires you to restart the server if there are errors found and if you want the Windows disk check utility to repair the errors. For this reason, Avaya does not recommend running the following checks during business hours. You should schedule a maintenance window to perform the checks.

### **To check for errors on hard disks**

- Before running the Windows disk check utility, perform a full system backup to avoid loss of data and messages.
- On the CallPilot server, double-click My Computer.
- Right-click the disk you want to check, and then click Properties.
- Click the Tools tab, and then in the Error-checking section, click Check Now.
- In the resulting dialog box, do not check either of the check disk options.
- Click Start.

The Windows disk check utility runs. If errors are detected, ensure a new drive is on hand as a spare, and then continue to the next step.

- On the disk with errors, rerun the Windows disk check utility (repeat steps 2 to 4 above), but this time, select both of the following check disk options:
  - Automatically fix file system errors
  - Scan for and attempt recovery of bad sectors
- Click Start.

A message asks you if you want the disk checking to occur the next time you restart the server. This is because the Windows disk check utility requires access to some Windows files that are available only during startup.

- Click Yes.
- Restart the server.

The Windows disk check utility runs as the server restarts.

11. Do one of the following:

- If the Windows disk check utility repairs the errors successfully, you can put the server back into service.
- If the Windows disk check utility cannot repair the errors, Avaya recommends you replace the affected hard disk with the spare hard disk. Follow the instructions for recovering a hard drive in Software Administration and Maintenance (NN44200-600).

---

## Checking LED/HEX displays for error indications

Frequency: Daily, or upon startup

LED errors display on the front panel of all platforms. LED errors can

- indicate the state of your server and help you troubleshoot startup problems
- indicate reduced server functionality
- indicate a recurring problem that can eventually result in loss of service

The following table outlines the LED color associated with your hard drive status for the 1005r, 1006r, 600r, 703t, 201i and 202i platforms. Observe the LEDs on the front panel of your server.

LED color	Hard drive status
Green/blinking green	Normal
Amber	Critical but recoverable condition. Often during a controlled condition such as a RAID split.
Red	Failure. This LED color is a major event, and you must attend to the server immediately.

The following table outlines the LED color associated with your hard drive status for the 1002rp platform. Observe the LEDs on the front panel of your server.

LED color	Hard drive status
Amber/blinking	Normal
Amber/solid	Critical condition
Amber/off	Failure

HEX errors only display on the 201i or 202i platform. HEX errors can

- indicate the state of your server
- indicate startup fault conditions
- indicate the highest severity event being experienced by the server

For a description of HEX display codes, see the <server model> Server Maintenance and Diagnostics Guide.

For a description of LED error indications and how to troubleshoot them, see the Troubleshooting Reference Guide (NN44200-700) and the Server Maintenance and Diagnostics Guide (for your server type).

---

## Monitoring event logs for Critical or Major events

Frequency: Daily

You can detect many potential hardware problems if you regularly monitor events and alarms. The section [Monitoring event logs for Critical and Major events](#) on page 24 in the previous chapter describes this preventative maintenance task.

For more information specific to hardware alarms and events, see the following guides:

- Administrator Guide (NN44200-601)
- Server Maintenance and Diagnostics Guide (for your server type)

---

## Maintaining server parts and cabling connections

Ensure the server parts on your CallPilot server function properly as described in the tasks in the following sections.

---

## Checking fans and power supplies for proper operation

Frequency: Monthly, or upon startup

If fans do not operate properly, the server can overheat. Overheating can cause physical damage to the server power supply.

When a fan fails, other fans will increase in speed to compensate for the loss of airflow. This increase in speed results in a significant increase in noise. If your system appears to be extremely noisy, there is likely a serious fan failure.

1005r, 1006r, and 600r	An amber or red LED signals power supply failures or fan failures. Check the functionality by opening the lid and visually inspecting the fans. If a fan fails, the others pick up speed and the server is extremely noisy. Also, when the lid is open, there is another lid that covers the fans inside. Remove that lid by unscrewing the blue thumbscrew and inspect the PCB SMD LEDs corresponding with each fan. If a LED is on, it indicates that the corresponding fan is faulty.
1002rp	A red LED signals power supply failures or fan failures. A combination of red LEDs on the front panel indicate the status of the fan or power supply. For example, if a power LED and fault LED are illuminated, then the problem is with the power supply. Similarly, if a fan LED and a fault LED are both illuminated, the problem is with the fan. To check, look at the back panel and the LED corresponding to the faulty supply will be red (instead of green).
703t	An amber or red LED signals power supply failures or fan failures. Check the functionality by opening the side lid and inspecting the individual fans.
201i or 202i	There are no fans on the 201i.

---

## Cleaning fan filters

Frequency: Every six months

 **Note:**

The 1002rp platform is the only platform with fan filters. For all other platforms, ensure the intake grill is free of dust and dirt.

Dirty fan filters reduce the flow of air around the server components and cause overheating.

### Cleaning fan filters

1. Carefully remove the front panel.
2. Visually inspect the fan filters or intake grill for dust or dirt.
3. Either wipe the filters with a cloth or blow on the filters to remove the dust or dirt.

---

## Cleaning tape drive heads

Frequency: Every six months, or every time the tape LED indicates cleaning is required.

The tape drive (Tandberg SLR5 and greater) LED (third LED from left) turns amber when cleaning is required.

1. Insert the cleaning cartridge.  
The cleaning procedure starts automatically.
2. Remove the cleaning cartridge from the drive when the cleaning operation is complete (the LED indicator light returns to normal and is no longer amber).
3. Store the cleaning cartridge in a protective container for future use.

---

## Maintaining RAID drives

Redundant Array of Independent Disks (RAID) is a technology that can combine two or more drives for fault tolerance and continuous service. Ensure your RAID operates properly by performing the tasks described in the following sections.

---

## Checking the status of RAID disk packs

Frequency: Weekly

Weekly or bi-weekly, ensure you check the status of the RAID disk packs. If RAID disks are not functional or the main disks fail, the server stops functioning.

1002rp and 703t	If critical issues with the drives occur, the RAID emits a beep. Media errors do not emit a beep.
1005r	This server does not emit a beep if a problem occurs. In CallPilot 5.0, 1005r errors are monitored by the front LEDs. The LEDs will turn amber in color if there are major or critical alarms. You need to check the status of the RAID packs using Power Console Plus. In CallPilot 4.0, errors can also be monitored by Intel ISM.

1006r	This server emits a specific sequence of beeps when certain problems occur.
201i, 202i, and 600r	RAID is not available on the 201i, 202i, or 600r.

For more information and to troubleshoot errors, see the Server Maintenance and Diagnostics Guide for your server type and the Troubleshooting Reference Guide (NN44220-700).

---

## Checking the consistency of RAID drives

Frequency: Avaya strongly recommends you check the consistency of RAID drives every six months.

Performing a consistency check on the RAID drives is optional. The check ensures that the data on the drives is identical. If errors are found, they are corrected automatically.

Avaya strongly recommends that you complete a consistency check before you split the RAID system pack. If possible, perform the consistency check the day before the scheduled maintenance. A good data backup on an offline drive is important if you need to revert to the CallPilot system from an unsuccessful upgrade or update.

 **Note:**

The consistency check can take up to two hours to complete and does not affect system performance.

### To perform a consistency check on a 703t, 1002rp, 1005r server

1. Open Power Console Plus. Click Start > Programs > Power Console Plus > Launch Client.

The MegaRAID Power Console Plus Server Selection window appears.

2. Ensure that you select Full Access under the Access Mode section, and then click OK.

The MegaRAID Power Console Plus window appears, displaying the Logical View of the Physical Devices and the Logical Devices. The status bar at the bottom of the window indicates that RAID channels are being scanned. When scanning is complete, the window refreshes and the Physical and Logical Devices window appears.

3. In the Logical Devices section, right-click the logical drive, and then choose Check Consistency from the shortcut menu.

The Check Consistency status window appears. You are informed when the check is finished. If any errors are found, a window with an error message appears.

4. Select Configuration > Exit to close the MegaRAID console.

An end of session message appears.

5. Click OK.

For more information about checking the consistency of RAID drives, see the Server Maintenance and Diagnostics Guide for your server type.

### **To perform a consistency check on a 1006r server**

1. Launch the RAID Web Console. Click Start > Programs > RAID Web Console 2 > StartupUI.
2. Enter the same credentials used for Windows login and ensure that Login Mode >Full Access is selected.
3. At the top of the Physical tab window, right-click the RAID Controller and select Schedule Consistency Check.
4. In the Schedule Consistency Check dialog box, enter the desired settings and clickOK.

The Check Consistency status window appears.

For more information about checking the consistency of RAID drives, see the Server Maintenance and Diagnostics Guide for your server type.

---

## **Ensuring RAID audible alarm is enabled on 1002rp and 703t**

Frequency: Monthly

1002rp and 703t (the 1005r has no audible alarm):

1. Open Power Console Plus. Click Start > Programs >Power Console Plus > Launch Client.  
The MegaRAID Power Console Plus Server Selection window appears.
2. Ensure that you select Full Access under the Access Mode section, and then click OK.
3. Under the menu item Adaptor, scroll down to Alarm Control to enable, disable, or silence the RAID alarm.

---

## Ensuring RAID audible alarm is enabled on the 1006r

1. Launch the RAID Web Console. Click Start > Programs > RAID Web Console 2 > StartupUI.
2. Enter the same credentials used for Windows login and ensure that Login Mode > Full Access is selected.
3. Right-click the RAID Controller at the top of the Physical tab window and select Enable Alarm.

---

## Checking the hard drive for media errors using the RAID Windows software

Frequency: Monthly

Media errors can indicate that a hard drive is failing. If the number of media errors appear to be increasing, consider replacing your drive. Using Power Console Plus, you can view the number of media errors by clicking on each individual drive and selecting properties.

### To check the hard drive on the 703t, 1002rp, or 1005r server

1. Open Power Console Plus. Click Start > Programs > Power Console Plus > Launch Client.
2. Ensure that you select Full Access under the Access Mode section, and then click OK.
3. Right-click each drive, and then and select Properties.

If your drive has media errors, they appear here.

For more information, see the Server Maintenance and Diagnostics Guide (for your server type).

### To check the hard drive on the 1006r server

1. Launch the RAID Web Console. Click Start > Programs > RAID Web Console 2 > StartupUI.
2. Enter the same credentials used for Windows login and ensure that Login Mode > Full Access is selected.
3. Click each drive and view the Properties on the right. Properties.

If your drive has media errors, they appear here.

Checking the hard drive for media errors using the RAID Windows software

For more information, see the Server Maintenance and Diagnostics Guide (for your server type).

Routine maintenance tasks: hardware maintenance

## Index

---

### C

customer service .....[7](#)

---

### D

distributor .....[7](#)  
documentation .....[7](#), [9](#)  
    map .....[9](#)

---

### F

Flight Recorder

archiving logs .....[25](#)  
deleting archives .....[26](#)  
downloading archives .....[26](#)  
viewing archive statistics .....[26](#)

---

### R

reseller .....[7](#)

---

### T

training .....[7](#)

