CallPilot 5.1 - Distributor Technical Reference

Introduction

This Distributor Technical Reference (DTR) bulletin provides information that supplements the formal documentation for the purpose of installing, upgrading, and supporting Avaya CallPilot® Release 5.1 (build 05.01) systems. It provides updated procedures, limitations, known problems, workarounds, and documentation addendum. This is an important information resource for Business Partner field operations and support personnel involved with CallPilot 5.1.

For more details on feature installation and operation, refer to the CallPilot 5.1 customer documentation.

This document, as well as other customer documentation, may be updated periodically as needed. It's recommended to always reference the Avaya Support Portal website for the latest information in updated NTPs or other documents. The CallPilot page can be directly accessed from: https://support.avaya.com/products/P0712/avaya-callpilot/

Avaya reserves the right to add, delete, or change features and packages in accordance with contractual obligations.

*Avaya and the Avaya logo are trademarks of Avaya, Inc.

LOTUS NOTES is a trademark of IBM Corporation.

PENTIUM is a trademark of Intel Corporation.

MICROSOFT EXCHANGE, MS-DOS, INTERNET EXPLORER, OUTLOOK 97, OUTLOOK 98, OUTLOOK 2000, OUTLOOK 2002 (XP), OUTLOOK 2007, OUTLOOK 2010, OUTLOOK 2013, OUTLOOK EXPRESS, WINDOWS 95, WINDOWS 98, WINDOWS NT, WINDOWS 2000, WINDOWS XP, WINDOWS VISTA, WINDOWS 7, WINDOWS SERVER 2000, WINDOWS SERVER 2003, and WINDOWS SERVER 2008 are trademarks of Microsoft Corporation.

NETSCAPE COMMUNICATOR is a trademark of Netscape Corporation.

NOVELL GROUPWISE is a trademark of Novell Corporation.

EUDORA PRO is a trademark of Qualcomm Corporation.

pcANYWHERE32 is a trademark of Symantec Corporation

Revision history

Revision Number / Date	Type of Review / Reason(s) for Issue	Author
December 3, 2012	Initial release of the 5.1 DTR in conjunction with General Availability (GA).	Roger Brassard
1.0 / October 11, 2013	Updated to reflect changes and improvements as per Service Update 2.	Roger Brassard
2.0 / September 12, 2014	Updated to reflect changes and improvements as per Service Update 3.	Roger Brassard

Table of contents

1 The Distributor Technical Reference Bulletin

1.1 Purpose

The purpose of the Distributor Technical Reference bulletin (DTR) is to provide the user with information for CallPilot 5.1 that is not covered by the NTP documentation supplied with the system. This DTR is intended for use in conjunction with the latest CallPilot 5.1 (05.01) software CDs/DVDs. Refer to the complete listing in CallPilot Software.

1.2 What's in CallPilot 5.1 and Available in this Release

CallPilot 5.1 includes all enhancement and corrective content as delivered in prior releases up-to and including CallPilot 5.0/Service Update 11 plus the following additional new items:

IT-centric compatibility updates:

- **Operating System for customer provided web server**
    - Windows 2008 Server (32-bit and 64-bit, standard edition)
    - Windows 2008 Server R2 (64-bit, standard edition)
    - Values: Longer life-cycle/support from Microsoft; eliminates need to re-install newer servers with older OS
- **Virtualization of customer-provided web server**
    - VMWare ESXI 3.5 and 5.1
    - Values: Aligns virtual environment with other applications likely to be installed on that same customer web server (e.g. Contact Center)
- **Operating System for Microsoft Active Directory integration (LDAP Sync)**
    - Windows 2008 Server (32 bit, standard edition)
    - Values: Longer life-cycle/support from Microsoft; eliminates need to re-install newer servers with older OS
- **Desktop Messaging/E-mail environments**
    - Microsoft Outlook 2010/64-bit (via new native 64-bit client)
    - GroupWise 2012
    - Values: Longer life-cycle/support from Microsoft and Novell
- **Desktop Messaging/Virtualization environments**
    - Citrix XenApps 6
    - Values: Improved performance; longer life-cycle/support from Citrix
- **Web-Browsers:**
    - Firefox 11 (for MAC and Windows)
    - Safari 5 (for MAC)
    - Google Chrome 18 (for MAC and Windows)
    - Values: Expanded browser support enhances usability /flexibility
- **Anti-Virus Applications (for use on the CallPilot server)**
    - McAfee 8.8
    - Symantec EndPoint Protection 12
    - Value: Adopts newer environments for increased security and optimal protection

Unified Messaging Enhancements

- **Microsoft Outlook 2010/64-bit**
    - 64-bit desktop client provides compatibility with Outlook 2010/64-bit and 64-bit OS environments.
    - Values: Eliminates the need to run in "compatibility" mode and provides optimal performance as a true 64-bit application
- **Desktop Messaging Offline Mode**
    - Eliminates recurring "check" for online condition
    - Value: Minimizes prompting to user, simplifying operation while offline
- **Message forwarding rule (MFR) enhancements**
    - Option to choose MFR WAV file encoding type
    - Value: Improves compatibility with mobile devices, allowing playback of messages using a broader range of codecs
- **Customizable "Remote Text Notification" message header**
    - Administrator or User defined header information
    - Value: Simplifies operation in multi-mailbox environments such as help-desks, saving respondents time/effort by knowing exactly which mailbox notified them
- **Password Change/Reset Service localized in French**
    - Language selection on login page allows users to quickly/easily choose between English and French
    - Value: Extends key money-saving services to broader marketplace; or comply with provincial law
- **My CallPilot Enhancements**
    - Increased Browser support, adding Google chrome and newer versions of others
    - Value: Greater flexibility for using common-place browsers
- Reporter Enhancements
    - No longer requires specific versions of Java Run-Time Edition for reports
    - Value: Reduced software requirements on user PCs; greater flexibility for anywhere reporting

Administrative Enhancements

- **Message Forwarding Rule Search**
    - MFR search capability allows for easier identification of users configured with this capability
    - Values: Simplified administration

1.3 What’s included in CallPilot 5.1 Service Update 2 (SU02)

Service Update 2 (SU02) includes corrective content for newly found field and lab found issues, in addition to all content from prior updates. Reference the appendices in this document or the readme and verinfo text files within the various component updates for details.

In addition to corrective code, SU02 also delivers the following additional elements:

- CallPilot Server
    - CPU optimization to improve system performance on 1006r servers
    - Improved memory management for 1002rp T1/SMDI systems
    - Numerous error/event codes updated for increased clarity/understanding
    - Enhanced Geographic Redundancy operation
    - Improved system operation and resiliency
- CallPilot Manager/Reporter
    - Compatibility with Windows 8 (x32 and x64 editions) OS environment
    - Compatibility with Internet Explorer 10
    - Enhanced report generation and scheduling capabilities
    - Improved operation with Windows Server 2008 (32-bit, 64-bit, and R2/64-bit standard editions) when hosted from a customer-provided web-server
    - Improved Configuration Wizard operation
    - Improved online help operation when using Google Chrome or Safari
    - Improved and simplified operations with directory-entry users
- Application Builder
    - Compatibility with Windows 8 (x32 and x64 editions) OS environment
- Desktop Messaging
    - Compatibility with Microsoft Outlook 2013 (x32 and x64 editions)
    - Compatibility with Windows 8 (x32 and x64 editions) OS environment
    - Improved operation and user experience when listening to longer messages via client
    - Enhanced guardrails to prevent installing/upgrading desktop messaging 64-bit with Outlook 32-bit
- My CallPilot
    - Compatibility with Windows 8 (x32 and x64 editions) OS environment
    - Compatibility with Internet Explorer 10 (requires “Compatibility View” be enabled)
    - Improved online help operation when using Google Chrome or Safari
    - Improved operation when using non-English languages

1.4 What's new in CallPilot 5.1 Service Update 3 (SU03)

Service Update 3 (SU03) includes corrective content for newly found field and lab found issues, in addition to all content from prior updates. Reference the appendices in this document or the readme and verinfo text files within the various component updates for details.

In addition to corrective code, SU03 also delivers the following additional elements:

- CallPilot Server
    - Improved memory management
    - Updated GR synch status monitor for increased accuracy and improved COS check utility
    - Improved database operations when performing backup/restore
    - Enhanced inter-operability with Exchange 2010/2013
    - Tighter security
        - Link Injection / Cross-Site Request Forgery (GRIP #12965)
        - Cross Site Scripting vulnerability (GRIP #12964)
    - Several error/event codes updated for increased clarity/understanding
- CallPilot Manager/Reporter
    - Auto-add enhanced to add e-mail addresses for Password Change/Reset service
    - Advanced Search enhanced for additional fields
    - Improved sorting options
    - Tighter security (aligning with similar improvements above
    - Improved connectivity performance between servers
    - Improved "Help" compatibility with Internet Explorer
- Desktop Messaging
    - Improved compatibility with Outlook 2013 when installed as part of Office 365
    - Enhanced support for server names >30 characters
- My CallPilot
    - Improved operation within Chinese Mandarin language
    - Improved compatibility with Internet Explorer 10

1.5 Supported Operations

1.5.1 Features on Controlled Release

The following is a list of 5.1 features that are on controlled release.

- Email-by-Phone languages other than Dutch, English, French, German, Italian, Russian, and Spanish, (using either Western European ISO-8859-1 or UTF-8 message encoding)

1.5.2 Switch Integration supported

The following switch integrations are supported:

- Meridian 1, Option 11C through 81C family of switches
- Communication Server 1000 family of switches
- Meridian SL-100 (Line-side T1 requires NT5D11 rev-5 and later)
- Communications Server 2000, 2100 (Line-side T1 requires NT5D11 rev-5 and later)
- DMS-100/CPE Centrex (Line-side T1 requires NT5D11 rev-5 and later)
- Communications Manager 6.2 (and later) via CS 1000 R7.5 or R7.5 and Session Manager
  - Reference Configuration Note CN88600

1.5.3 Switch Integrations deferred

- None

1.5.4 Server Hardware Platforms supported

The following CallPilot server platforms offered for new, foundation, and migration systems:

- 202i IPE (ELAN)
  - Small capacity in-skin server (IPE form factor)
  - 32 MPU / Channel capacity with 350 hours storage
  - Pricing is similar to 201i IPE but newer technology
  - Idea for Option-11C/Mini/CS 1000 solution for both Unified Messaging and Contact Center voice prompts
- 1006r Rackmount (ELAN/MGate)
  - High-end rack mount server (703t, 1002rp, or 1005r replacement)
  - 288 MPU/192 channel capacity with 2400 hours storage
  - 2nd server for high availability – manual/automatic failover
  - Avaya Aura™ Messaging ready – A platform for the future
- 1002rp Rackmount (T1/SMDI)
  - High-end rackmount server (1001rp T1/SMDI replacement)
  - 288 MPU/192 channel capacity with 2400 hours storage

1.5.5 Server Hardware Platforms sustained

The following CallPilot server platforms are sustained and no longer available for new/migration system purchases. However, each fully supports software release upgrades to 5.1.

- CallPilot 5.x Sustained Servers *
    - 201i IPE
    - 703t Tower
    - 600r Rackmount
    - 1002rp Rackmount (for CS 1000-integration only)
    - 1005r Rackmount (for CS 1000-integration only)

1.5.6 Server and Client Upgrades supported

Upgrades to CallPilot 5.1 are supported directly from CallPilot release 5.0. Prior releases 2.02, 2.5, 3.0 and 4.0 must first upgrade to release 5.0 before proceeding to 5.1. Minimum SU levels required are: 2.02/SU04 and 2.5/SU02.

Upgrading to CallPilot 5.1 from CallPilot version 1.07 requires an upgrade from 1.07 to 2.02/SU04 (ELAN integration) or 1.07 to 2.5/SU02 (T1/SMDI integration) and then to 5.0 before applying the 5.1 update.

1.5.7 CallPilot 5.0/5.1 Keycode operations

CallPilot 5.0 and 5.1 utilize the same keycodes. No new keycode is required when upgrading from 5.0 to 5.1. Upgrades from previous releases will require a new 5.x keycode, provided by order Management as part of purchasing the release upgrade.

1.6 About Customer Documentation

The starting point for all CallPilot activities is the customer NTP documentation and Offline Help, available through the Avaya Partner and/or Support Portal websites using these links:

Sales Portal:	http://www.avaya.com/salesportal
Partner Portal:	http://www.avaya.com/partner
Support Portal:	http://support.avaya.com
CallPilot page:	https://support.avaya.com/products/P0712/avaya-callpilot/

The NTP documentation can be viewed on any PC using Adobe Acrobat Reader 5.0 or later.

Note: These documents, as well as other customer documentation, were updated to include the content within this new release. They may also be updated periodically as needed. It's always recommended to reference the Avaya Partner Portal website for the latest information in updated NTPs, Offline Help, or Release Notes documents.

1.6.1 High Availability Configuration Video

A configuration video is available for download from the Support portal webpage. This self-paced tutorial covers installation and configuration of a CallPilot High Availability system, plus describes other High Availability concepts and terminology.

This CallPilot and Contact Center (Symposium) Integration is not covered in this video. For integration details, please refer to the Feature Information & Limitations/Contact Center Interoperability section of this document.

The instructional video is located on the CallPilot page, under the Downloads sub-heading. A direct link to the configuration video is available at:

https://support.avaya.com/css/SAFE/downloads?downloadId=9459

1.6.2 High Availability / Contact Center supplemental training

A supplemental training course (#6350W) is available for CallPilot High Availability configurations (including with Contact Center integration). This course complements the above noted video and leader-led courses, de-mystifying some of the complexity with implementing a High Availability solution.

This self-paced tutorial covers installation and configuration of a CallPilot High Availability system, plus describes other High Availability concepts and terminology. Contact Messaging Product Management (brassard@avaya.com) for access to this course download.

1.7 Software Updates/Enhancements

After completing the upgrade, verify whether there are any additional PEPs to be installed. Refer to PEP/Service Update application overview for additional information.

1.8 Localized Media

The table below summarizes localized CallPilot 5.1 media available as of the date of this document:

Language	Voice Prompts	Desktop Messaging	My CallPilot	Speech Activated Messaging	E-mail by Phone	End User Docs
Arabic	✓					
Cantonese	✓	✓ (Traditional)				✓ (Traditional)
Catalan	✓					
Czech	✓					
Danish	✓					✓
Dutch	✓	✓			✓	✓
English, American (US)	✓	✓	✓	✓	✓	✓
English, Australian	✓	✓	✓		✓	✓
English, Canadian	✓	✓	✓	✓	✓	✓
English, Irish	✓	✓	✓		✓	✓
English, UK (female)	✓	✓	✓	✓	✓	✓
Finnish	✓					
French, Canadian	✓	✓	✓	✓	✓	✓
French, European	✓	✓	✓	✓	✓	✓
German	✓	✓	✓	✓	✓	✓
Greek	✓					✓
Hebrew	✓					
Hungarian	✓					
Italian	✓	✓	✓	✓	✓	✓
Japanese	✓	✓		✓		✓
Korean	✓					
Mandarin, PRC	✓	✓ (Simplified)				✓ (Simplified)
Mandarin, Taiwanese	✓	✓ (Traditional)				✓ (Traditional)
Norwegian	✓					
Polish	✓					
Portuguese	✓					
Portuguese, Brazilian	✓					✓
Russian	✓				✓	✓
Slovak	✓					
Spanish, Castilian	✓	✓	✓			✓
Spanish, Latin American	✓	✓	✓		✓	✓
Swedish	✓					
Thai	✓					
Turkish	✓					

2 Product Requirements

2.1 CallPilot 5.1 Compatibility

The following tables define CallPilot 5.1 compatibility with other products and environments it is likely to encounter.

Product / Function	CallPilot 5.1 Compatibility
Meridian Mail	• Co-existence with Meridian Mail on Meridian 1 or Communication Server 1000 family is supported. Networking to Meridian Mail available with AMIS-A and Enterprise networking protocols or via VPIM with Meridian Mail Net Gateway.
Meridian Mail Reporter	• Cannot be used to generate reports from a CallPilot server. • Meridian Mail Reporter only supports Meridian Mail and CallPilot Reporter only supports CallPilot.
Custom Controlled Routing (CCR)	• Co-existence of CCR and CallPilot on the same Meridian 1 is supported. • CallPilot does not support CCR command: Give IVR.
Message Networking (Releases 5.2 and 6.3)	• CallPilot 5.1 is compatible
Symposium Call Center Server 4.2, 5.0, and Contact Center 6.x and 7.0 (standard and H/A); Avaya Aura Contact Center 6.x (AML integration; standard and H/A)	• Co-existence with Contact Center/Symposium Call Center Server or Express on the same M1/CS 1000 and ELAN is supported. • CallPilot 5.1 supports Symposium Call Center Server and Contact Center (AML) integration for voice processing script commands: “Give IVR”, “Give Controlled Broadcast”, “Collect Digits”, “Play Prompt”, and “Open…End Voice Session”. • CallPilot 5.1 (non H/A) supports Symposium Express 4.2 integration for voice processing script commands “Give IVR”. • CallPilot 5.1 High Availability is only supported with Contact Center 6.x and Contact Center 7.0 (CCMS/AACC AML versions).
Microsoft Office 2002 (XP), 2003, and 2007, 2010 and 2013 (32-bit and 64-bit)	• CallPilot 5.1 Desktop Messaging client is compatible • Outlook 2010/64-bit requires use of 64-bit client. • Outlook 2013 requires use of 05.01.02.06 or later client.
Line-Side interface	• Line-side T1 interface card (NT5D11) requires version 5 or later for proper integration/functionality.
Remote Control applications	• Symantec pcAnywhere, Microsoft RDC, WebEx, LogMeIn Rescue, and RealVNC
Avaya Aura® Messaging	• Co-existence with Avaya Aura® Messaging on Communication Server 1000 family is supported.

2.1.1 Migration from Meridian Mail / Database compatibility

Migration from Meridian Mail systems to CallPilot 5.1 is supported using the Meridian Mail migration utility tape NTUB25AC (available within NTUB24BA Migration Package). This supports migration from all Meridian Mail MM11, MM12, and MM13 releases for all Meridian Mail platforms except the MSM and Card Option running MM13.11.2. It is required for all Meridian Mail releases including MM13.14 as this tape supersedes the migration utility available in the TOOLS level.

Notes:

1. Previous 1.07 versions of the migration utility NTUB24AA, NTUB24AB or NTUB24AC cannot be used with CallPilot 5.0. The Migration guide should be consulted for limitations.
2. CallPilot requires use of the NTRB18CA (DS30) and NTRB18DxE5 (CAT-5E) MGate cards for connectivity. Systems migrated from Meridian Mail must ensure only the updated MGate cards are used.
3. Unlike Meridian Mail where calls were directly routed to the main ACD-DN (queue) feeding Meridian Mail ports, a CDN is used to route calls to CallPilot. It is imperative that all calls be routed through the CDN and not directly to the ACD-DN associated with CallPilot channels. See the Migration guide for details.

2.1.2 Application Builder client / Operating System (OS) compatibility

Operating Systems:	2.02/2.5	3.0	4.0	5.0	5.1
Windows 2000 Professional (ISO-8859-1, Latin-1 character set versions)	Note 1	Note 1	Note 1	Note 1	Note 1
Windows 2000 Server, Advanced, or Data Center Server					
Windows XP Home					
Windows XP Professional	✓	✓	✓	✓	✓
Windows XP Professional x64 Edition				Note 5	✓
Windows Vista				Note 3	✓
Windows Vista x64 Edition				Note 5	✓
Windows 7				Note 4	✓
Windows 7 x64 Edition				Note 5	✓
Windows 8					Note 6
Windows 8 x64 Edition					Note 6, 7
Windows Server 2003					
Macintosh OS 9.0 or 9.1					
Macintosh OS X					

Notes:

1. ISO-8859-1 (Latin-1) character sets cover most West European languages including but not limited to: English, French, Spanish, Catalan, Basque, Portuguese, Italian, Albanian, Rhaeto-Romanic, Dutch, German, Danish, Swedish, Norwegian, Finnish, Faeroese, Icelandic, Irish, Scottish, Afrikaans, and Swahili.
2. CallPilot 5.1 is backward compatible for use with CallPilot 2.5/SU02 and later servers.
3. Requires version 05.00.41.27 (available as PEP CP500S02G27A) or later.
4. Requires version 5.00.41.62 (available as PEP CP500S08G08A) or later.
5. Requires version 5.00.41.76 (available as PEP CP500S10G04A) or later.

6. Requires version 5.01.02.02 (available as PEP CP501S02G02A) or later.
7. Windows 8 (64-bit) requires 32-bit version CallPilot Player be installed. Refer to wi01090235.

2.1.3 Desktop Messaging / Groupware compatibility

CallPilot Desktop Messaging and My CallPilot support the following Groupware e-mail clients, Internet mail clients, Web clients, and thin clients. Please refer to the “verinfo.txt” file contained with the CallPilot Desktop Messaging and My CallPilot package for the latest details on supported sub-releases of the clients. Note that sub-releases are generally supported. However, Avaya reserves the right to suspend support for a sub-release which introduces a problem.

Groupware E-mail clients	**2.50.06.17 and later**	**04.04.04.18 and later**	**CallPilot 5.0**	**CallPilot 5.1**
Microsoft Outlook 2000	✓	✓		
Microsoft Outlook 2002 (XP)	✓	✓	✓	✓
Microsoft Outlook 2003	✓	✓	✓	✓
Microsoft Outlook 2007			✓	✓
Microsoft Outlook 2010 (32-bit)			05.00.41.112 and later	✓
Microsoft Outlook 2010 (64-bit)				✓
Microsoft Outlook 2013 (32-bit)				05.01.02.06 and later
Microsoft Outlook 2013 (64-bit)				05.01.02.06 and later
Lotus Notes 5.0x	✓			
Lotus Notes 6.0.5	✓	✓	✓	✓
Lotus Notes 6.5	✓	✓	✓	✓
Lotus Notes 7.0		✓	✓	✓
Lotus Notes 8.0			✓	✓
Lotus Notes 8.0.2			5.00.41.67 and later	✓
Lotus Notes 8.5			5.00.41.96 and later	✓
Novell GroupWise 6.0x	✓			
Novell GroupWise 6.5	✓	✓	✓	✓
Novell GroupWise 7.0		✓	✓	✓
Novell GroupWise 8.0			5.00.41.96 and later	✓
Novell GroupWise 2012 SP1				✓
Internet Mail clients	**2.50.06.17 and later**	**04.04.04.18 and later**	**CallPilot 5.0**	**CallPilot 5.1**
Microsoft Outlook Express 5.x	✓			
Microsoft Outlook Express 6.x	✓	✓	✓	✓
Windows Vista Mail			✓	✓
Microsoft Outlook 2000 (XP) (Internet Mail Mode)	✓	✓		

Internet Mail clients	**2.50.06.17 and later**	**04.04.04.18 and later**	**CallPilot 5.0**	**CallPilot 5.1**
Microsoft Outlook 2002 (XP) (Internet Mail Mode)	✓	✓	✓	✓
Microsoft Outlook 2003 (Internet Mail Mode)	✓	✓	✓	✓
Microsoft Outlook 2007 (Internet Mail Mode)			✓	✓
Microsoft Outlook 2010 (Internet Mail Mode)			05.00.41.112 and later	✓
Microsoft Outlook 2013 (Internet Mail Mode)				5.01.02.06 and later
Netscape 6.2x	✓	✓		
Netscape 7.0, 7.1, and 7.2	✓	✓		
Qualcomm Eudora Pro 5.x	✓			
Qualcomm Eudora Pro 6.0	✓	✓		
Qualcomm Eudora Pro 6.1	✓	✓		
Thin clients	**2.50.06.17 and later**	**04.04.04.18 and later**	**CallPilot 5.0**	**CallPilot 5.1**
Citrix MetaFrame 1.8 on Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server	✓			
Citrix MetaFrame XP (Standard, Enterprise, or Advanced Editions) on Windows 2000 Server, Windows Server 2003 (All Editions)	✓	✓	✓	✓
Citrix MetaFrame Presentation Server 3.0 on Windows Server 2003 (All Editions)		✓	✓	✓
Citrix MetaFrame Presentation Server 4.0 on Windows Server 2003 (All Editions)			✓	✓
Citrix XenApps 6 on Windows 2008 R2 Server				✓

Notes:

1. Desktop Messaging client versions 1.05/1.06/1.07 are not supported for use with 5.1, 5.0, 4.0, 3.0, 2.5 or 2.0x servers
2. Desktop Messaging version 5.1 is not supported with 2.02 and earlier servers

2.1.4 Desktop Messaging client / Operating System (OS) compatibility

Desktop Messaging clients are supported for use on the following Operating Systems:

Operating Systems	**2.50.06.17 and later**	**04.04.04.32 and later**	**CallPilot 5.0**	**CallPilot 5.1**
Windows 2000 Professional	✓	✓	✓	✓
Windows 2000 Server, Advanced, or Data Center Server				
Windows XP Home				
Windows XP Professional	✓	✓	✓	✓
Windows XP Professional (x64 Edition)			5.00.41.154 and later	✓
Windows Vista			✓	✓
Window Vista (x64 Edition)			5.00.41.154 and later	✓
Windows 7			5.00.41.97 and later	✓
Windows 7 (x64 Edition)			5.00.41.154 and later	✓
Windows 8				5.01.02.06 and later
Windows 8 (x64 Edition)				5.01.02.06 and later
Windows Server 2003				
Macintosh OS 9.0 or 9.1				
Macintosh OS X				
Linux				

2.1.5 My CallPilot / Browser Compatibility

My CallPilot Web Messaging supports the following Internet browsers:

Internet Browsers	**2.50.06.23 and later**	**04.04.04.20 and later**	**CallPilot 5.0**	**CallPilot 5.1**
Netscape 6.2x for Windows or Mac	✓	✓		
Netscape 7.0, 7.1, and 7.2 for Windows or Mac	✓	✓		
Microsoft Internet Explorer 5.x for Windows	✓			
Microsoft Internet Explorer 6.0 for Windows	✓	✓	✓	✓
Microsoft Internet Explorer 7.0 for Windows			✓	✓
Microsoft Internet Explorer 8.0 for Windows			5.00.41.111 and later	✓
Microsoft Internet Explorer 9.0 for Windows			5.00.41.154 and later	✓
Microsoft Internet Explorer 10 for Windows 8				5.01.02.06 and later
Firefox 2.0 for Windows			✓	
Firefox 11 for Windows				✓
Google Chrome 18				✓
Microsoft Internet Explorer 5.x for Mac	✓	✓		
Firefox 11 for Mac				✓
Google Chrome 18 for Mac				✓
Safari 1.3.2 for Mac			✓	
Safari 5.1.4 for Mac				✓
Mozilla 1.7.13 for Linux		✓	✓	✓
Firefox 2.0 for Linux		✓	✓	✓

Note:

1. Compatibility with Internet Explorer 9 and 10 requires "Compatibility View" be enabled.
2. Compatibility with IE10 on Windows 8 (64-bit) requires32-bit CallPilot Player is installed. Refer to wi01090235.

2.1.6 My CallPilot client / Operating Systems compatibility

My CallPilot clients are supported for use on the following Operating Systems:

Operating System	**2.50.06.23 and later**	**04.04.04.20 and later**	**CallPilot 5.0**	**CallPilot 5.1**
Windows 2000 Professional	✓	✓	✓	✓
Windows 2000 Server SP1 and above (w/ IIS 5)	✓	✓	✓	✓
Windows XP Professional	✓	✓	✓	✓
Windows Server 2003 (32-bit only, w/ IIS 6)	✓	✓	✓	✓
Windows Vista			✓	✓
Windows 7			5.00.41.111 and later	✓
Windows 8				5.01.02.06 and later
Windows Server 2008, Service Pack 1 (w/ IIS 7)			5.00.41.167 and later	✓
Windows Server 2008 R2 (x64 Edition), Service Pack 1 (w/ IIS 7)			5.00.41.167 and later	✓
Macintosh OS 9.0 or 9.1	✓	✓		
Macintosh OS X	✓	✓	✓	✓
Linux			✓	✓

Note:

1. Partial support for Mac OS X is supported with My CallPilot version 2.50.06.11 and later. No CallPilot Player, CallPilot Fax Viewer, or interaction with the TUI will be available. Listening to and viewing of CallPilot messages will be accessed via desktop only and handled by the resident audio player and picture viewer of the MAC OS.
2. Compatibility with Windows 8 (64-bit) requires32-bit CallPilot Player is installed. Refer to wi01090235.

2.1.7 My CallPilot server / OS/IIS and Browser compatibility

CallPilot 5.1 My CallPilot supports the following operating systems and browsers:

Product / Function	**CallPilot 5.0 Compatibility**
Server side details:	
Operating Systems	• Windows 2000 Server with Service Pack 1 or later (**Note:** Standard version only.) • Windows Server 2003 , Service Pack 1 or later (**Note**: Standard 32-bit version only) • Windows Server 2008, Service Pack 1 or later (**Note**: 32-bit and 64-bit versions, standard edition only) • Windows Server 2008 R2 (64-bit, standard edition)
Internet Service software	• Internet Information Server 5.0 (Service Pack 1 or later) • Internet Information Server 6.0 • Internet Information Server 7.0
Browsers	• Internet Explorer 6.x, 7.x, 8.x, 9x, and 10 (See note.) • Firefox 11 for Windows • Google Chrome 18 for Windows

Notes:

1. Localized browsers are not supported at this time.
2. Internet Explorer 9 and 10 require "Compatibility View" is turned on. Use the following steps:
    a. Launch Internet Explorer 9
    b. Within the "Address" bar, click the "Compatibility View" button
3. Internet Explorer 10 requires My CallPilot version 05.01.02.06 or later.

2.1.8 CallPilot Manager/Reporter stand-alone web server compatibility

The requirements for the stand-alone web server for installing CallPilot Manager (with or without CallPilot Reporter) and My CallPilot are as follows.

Supported Operating Systems	Supported
Windows NT 4.0 Server with SP6a and Microsoft Internet Information Server (IIS) 4	No
Windows 2000 Server with SP1-SP4 and Microsoft Internet Information Server (IIS) 5	No
Windows Server 2003 Standard Edition SP1 and Microsoft Internet Information Server (IIS) 6	Yes
Windows Server 2003 Web Edition SP1 and Microsoft Internet Information Server (IIS) 6	No
Windows Server 2003 Enterprise Edition SP1 and Microsoft Internet Information Server (IIS) 6	No
Windows Server 2003 Standard Edition SP2 and Microsoft Internet Information Server (IIS) 6	Yes
Windows Server 2003 Web Edition SP2 and Microsoft Internet Information Server (IIS) 6	No
Windows Server 2003 Enterprise Edition SP2 and Microsoft Internet Information Server (IIS) 6	No
Windows Server 2003 x64 Edition	Yes
Windows Vista (Standard and Enterprise Editions) and Microsoft Internet Information Server (IIS)	No
Windows 2008 Server (32-bit and 64-bit, Standard Edition)	Yes
Windows 2008 Server R2 (64-bit, Standard Edition)	Yes

Notes:

1. Operating System must be installed on the C: drive
2. Windows Server 2003 and 2008 web-servers require installation of .NET Framework 2.0 **PRIOR** to installation of CallPilot Manager/Reporter.
3. For proper operation of CallPilot Reporter, customer-provided web-servers should have the following features/services enabled:
    a. Common HTTP features
    b. ASP.NET (and all other services it requires to be installed)
    c. Classic ASP

Note: A part of these features may or may not be installed/enabled by default depending on OS version/image.

2.1.9 Platform Hardware/BIOS/Software requirements

This list is intended for use in addition to the requirements captured in the current issue of the CallPilot 5.1 NTP documentation.

Platform	Component	Version
201i	BIOS	6.0.3
202i	BIOS	27
703t – Shipped with CP3.0 – CP4.0	BIOS	16 Build 75
	Firmware	FRU SDR 5.5 BMC 1.18
703t – shipped with CP2.02 – CP4.0	BIOS	7 Build 64 [2]
1002rp	BIOS [1]	NNCXUA07
600r	BIOS	Intel P9.10 Build 40
	Firmware	FRU/SDR 6.6.3 BMC 2.40
LSI MegaRaid 1600	Firmware	111U [1]
LSI MegaRaid 320-2	Firmware	1L37 [3] (if 1002rp)
LSI MegaRaid 320-1 (1005r only)	Firmware	1L37 or 1L51 [3]
1005r	BIOS	10 build 87
	Firmware	FRU/SDR 6.6.5 BMC 0.50
1006r	BIOS	BIOS50
	Firmware	BMC53
		FRU / SDR24
		ME 1.12
		RAID OPROM v1.40.92-0746
		HSC 2.15

Notes:

1. Please refer to the NTP Server Maintenance and Diagnostics guides for configuration details:
    a. NN44200-701 1002rp Rackmount
    b. NN44200-702 703t Tower
    c. NN44200-703 600r Rackmount
    d. NN44200-704 1005r Rackmount
    e. NN44200-705 201i IPE
    f. NN44200-708 202i IPE
    g. NN44200-709 1006r Rackmount
2. The 703t BIOS is not field upgradable. The BIOS currently residing on the 703t server is supported in CallPilot 5.0. If an upgrade is occurring from CallPilot version 2.02, Windows Server 2003 will need to be activated using the certificate of authenticity (COA) provided in the upgrade package. The process for activating Windows Server 2003 is as follows; Select "Change Product Key" tab; enter the COA from the Windows Server 2003 package sticker and a new Product ID will be generated, call the toll-free number and enter the New Product ID. Activation should be complete.
3. Refer to section 8.1.18 for details on upgrading the RAID firmware

2.1.10 Supported Customer LANs

Product / Function	CallPilot 5.1 Compatibility
10Base-T	All platforms
100Base-T	201i and 202i (IPE), 703t (Tower), 600r, 1005r and 1002rp (Rackmount) without additional hardware (see note)
1000Base-T	703t (Tower), 600r, 1005r, and 1006r (Rackmount)

Notes:

1. All platforms include 10/100Base-T Ethernet LAN NIC cards except 703t, 600r, 1005r, and 1006r which includes 10/100/1000Base-T Ethernet LAN NIC
2. Token Ring (4 or 16 Mbps) LAN is not supported in CallPilot 5.0.
3. ELAN must be configured the same as the switch configuration.
4. If a switch is used for ELAN or CLAN, “Spanning Tree” must be turned off.
5. CLAN should be configured for Auto-Detect.

2.1.11 Supported LAN/WAN Networking Protocols

CallPilot supports only TCP/IP (internet) networking protocols. Novell’s IPX/SPX protocol is not supported.

2.2 Operational Requirements

2.2.1 3rd-party Software and Hardware

The addition of any 3rd-party software or hardware to the CallPilot server is not supported other than tested, qualified, and approved anti-virus applications, remote-control applications, Adobe Acrobat Reader updates, and Microsoft security updates. Doing so can destabilize the system; degrade its mission of providing real-time call processing performance, and cause future upgrades to fail. Refer to Product Bulletin 99067 – *CallPilot Unauthorized Hardware and Software* for more information. For additional details, refer to bulletins:

- CallPilot Support for Anti-Virus Applications – <year>
- CallPilot Server Security Update – <year> (*details on Microsoft hotfix compatibility*)
- PAA-2010-0006-Global – *CallPilot Security Update – Adobe Reader*
- CallPilot Security Advisory – *Symantec pcAnywhere*

or published Product Change Notice or Product Security Advisory Alerts.

2.2.2 Software dongle installation

The CallPilot dongle must be properly installed in the server prior to accessing CallPilot Manager. High Availability systems, which consist of either two (2) 1005r servers or two (2) 1006r servers, have only one (1) dongle installed on the active server. Some management functions are restricted on the standby server.

2.2.3 Proper Power and Grounding

All CallPilot server installations (201i, 202i, 600r, 703t, 1002rp, 1005r, and 1006r) must follow the Meridian 1 and/or Communication Server 1000 and CallPilot NTP guidelines for proper power and grounding, specifically, adhering to the Single-Point Ground Reference requirement. Failure to follow these guidelines makes Meridian 1/Communication Server 1000/1000M/1000E and CallPilot susceptible to damage from electrical transients resulting from lightning and other power-ground disturbances.

The Single-Point Ground Reference includes all powered devices that attach directly to the PBX and its ancillary equipment. For a typical CallPilot installation, the following components are included:

- PBX
- CallPilot server
- Uninterruptible Power Supply (UPS) (if installed)
- Remote maintenance modem
- ELAN and CLAN hubs
- Administration/Maintenance PC (and associated monitor and printer)
- External DVD/CD-ROM and (201i and 202i IPE servers)
- External Tape drives (201i and 202i IPE, 600r, 1005r, and 1006r rackmount)
- External USB Disk drives (202i, 600r, 1005r, and 1006r servers)
- Contact Center (Symposium Call Center) Server (if installed)

As well, in CallPilot Rackmount server installations, the following supplemental information applies:

- Ensure the CallPilot server chassis and equipment racks are isolated from other foreign sources of ground
- Acceptable isolation methods include: isolation pads, grommet washers, chassis side rail strips and non-conducting washers, etc.
- Where other equipment is also installed in the same 19" rack, ensure that all equipment derives ground from the same service panel as CallPilot and the switch, whether or not the equipment is AC or DC powered.
- In DC-powered server installations, ensure the PDU (Power Distribution Unit for DC applications) is installed on the same rack as the CallPilot server. This is required since the main ground wire for the PDU is not insulated from the metal enclosure.
- The DC resistance of the system ground conductor, which runs from the switch to the main building ground, must be as close to zero as possible. The maximum total resistance on all runs within the building must not exceed 0.5 ohms, per NN44200-200 Planning and Engineering guide.

It's also highly recommended that a UPS be equipped on Tower/Rackmount installations.

Important Note: Adherence to a Single-Point Ground reference applies to all existing installed-base systems as well as new CallPilot server installations. Whether working on a new install or performing maintenance on an existing system, verifying the system is properly grounded can help avoid damage or system outage from electrical transients.

2.2.4 Shutdown/Restart required after PBX maintenance procedures

To ensure proper operation of the CallPilot server after performing a SYSLOAD or Parallel Reload of the PBX, the CallPilot server must be rebooted to ensure all resources are properly re-acquired. As well, when possible, it's preferred that the CallPilot server be taken offline during the maintenance procedure and then restarted once the PBX work has been completed.

To shut down the CallPilot system either of the following two (2) methods is supported: Use "Ctrl-Alt-Delete" or Start/Shutdown and select "Shutdown" from the Windows Security window. Then from the Shutdown Computer dialog box that appears, select either "Shutdown" or "Shutdown and Restart" as appropriate. Enter a reason for shutting down the Computer in the reason field.

2.2.5 201i IPE recommended handling procedures

To minimize data loss or damage to the drive media, when removing power from the 201i IPE server, ensure the system avoids excessive vibration until the hard drive heads have parked using the recommending handling procedure below. Refer to wi00678695.

1. Perform a shutdown
2. Remove power by gently unseating the server from the backplane
3. Allow the server to remain still for approximately 15 seconds. This allows the disk to spin down (i.e. stop rotating), allowing the heads to come safely to rest on the platter surface.
4. Remove the IPE server as handle as normal following ESD guidelines.

2.2.6 202i IPE recommended peripheral installation procedures for 61C/81C

When initially booting a 202i IPE system, ensure that USB peripherals and connection cable lengths are not excessive as this may potentially cause the USB signal driver to overload resulting in the HEX display to scroll "HOST" without video appearing.

In Large Meridian 1 (Option 61C/81C) installations wherein the Avaya supplied six (6) foot USB extension cables route from the 202i front faceplate to the switch rear I/O panel, it has been noticed that with a fully populated USB devices (Mouse, Keyboard, Modem, DVD drive, and Tandberg RDX backup device) the system may experience USB driver to overload and fail to boot.

To ensure failsafe power-up recovery in the event of a power failure, Avaya recommends to have only one (1) USB device connected full-time via the six (6) foot USB extension cable, typically, the backup device.

Avaya is investigating this overall concern and may make further product enhancements to rectify or may publish follow-up supplemental documentation clarifying the matter.

Note: This ONLY appears during initial product boot-up. Post power-on re-connection of the USB peripherals is valid and functional for both ports utilizing the six (6) foot USB cable extensions.

3 Meridian 1 switch requirements

NTP NN44200-302 – *Meridian 1 and CallPilot Server Configuration* Chapter 4 describes how to configure a Meridian 1 PBX to work with CallPilot. The following description is an addendum to this chapter, describing the specific Meridian 1 models supported, the supported X11 software releases, and the PEPs available for the various releases for proper CallPilot operation.

Section 3.1 lists the supported Meridian 1 models. Section 3.2 identifies the supported software releases. Section 3.3 lists required packages relevant to CallPilot. Section 3.4 provides a list of the available PEPs with a description of the issues addressed and its applicability to the system model and software release.

Note: **Information on the X11 software changes regularly.** For the most recent information on supported X11 software releases and PEPs refer to the Enterprise Solutions PEP Library (ESPL) website at: https://support.avaya.com/espl (all regions)

Note: If you are new to the ESPL website, you will need to register for a user ID/password. Please apply on-line or contact Channel Partner Account Manager.

3.1 Meridian 1 switches supported

Meridian 1 – Options 11C, 11C/Mini, 51C, 61C, 81, 81C

Note: The copper-connection Option 11C does not support ELAN, which is required for CallPilot.

3.2 Software Releases supported

Switch software releases supported: X11R25.40 and X11R25.40B

3.3 X11 Packages required for CallPilot 5.1

The following switch software packages are required to support CallPilot. Due to 25.40's LCM rating, if these packages are not already equipped, they cannot be added.

Pkg #	**Description**
41	ACDB (ACD Package B)
46	MWC (Message Waiting Center)
214	EAR (Enhanced ACD Routing)
215	ECT (Enhanced Call Treatment)
218	IVR (Hold in Queue for IVR)
247	Call ID
324	NGEN (CallPilot Connectivity) See next table
364	NMCE (CallPilot)
254	PHTN (Phantom TN)

Package 324 requirements	
Pkg #	**Description**
77	CSL (Command Status Link)
153	X25AP (Application Module Link – AML)
164	LAPW (Limited Access to Overlays)
242	MULI (Multi-User Login)
243	Alarm Filtering
296	MAT (Meridian Administration Tool)

3.4 X11 PEPs to support CallPilot 5.1

It is highly recommended to review the following bulletins located at: https://support.avaya.com/espl for supplemental PEPs that might be applicable.

- X11 Release 25.40/25.40B and DepList Integration Bulletin – CallPilot
- X11 Release 25.40/25.40B and DepList Integration Bulletin – CallPilot/SCCS Integration

4 Communication Server 1000 switch requirements

Communication Server 1000 (CS 1000) is a communications system that provides a single solution for telephony and data capabilities. CS 1000 provides a full suite of industry-leading voice features and uses global software. The software stream used on a CS 1000 is X21, which delivers software with equivalent features and functionality to Meridian 1 X11 25.30 and later. This software stream provides the same seamless integration between CallPilot and CS 1000 as between CallPilot and Meridian 1.

4.1 CallPilot Platforms Supported

- 201i and 202i IPE
- 703t Tower
- 600r, 1002rp, 1005r, and 1006r Rackmount

Please refer to NTP NN44200-312 CS 1000 and *CallPilot Server Configuration Guide –*, for further details on Communication Server 1000 and the installation and configuration of CallPilot with this switch.

4.2 Software Releases supported

- X21 release 3.0 and later

4.3 X21 Packages required for CallPilot 5.1

Pkg #	Description
41	ACDB (ACD Package B)
46	MWC (Message Waiting Center)
214	EAR (Enhanced ACD Routing)
215	ECT (Enhanced Call Treatment)
218	IVR (Hold in Queue for IVR)
247	Call ID
324	NGEN (CallPilot Connectivity) See next table
364	NMCE (CallPilot)
254	PHTN (Phantom TN)

Package 324 requirements	
Pkg #	**Description**
77	CSL (Command Status Link)
153	X25AP (Application Module Link – AML)
164	LAPW (Limited Access to Overlays)
242	MULI (Multi-User Login)
243	Alarm Filtering
296	MAT (Meridian Administration Tool)

All the above software packages are included in the Communication Server 1000 *Basic Software Service* package by default, for each CS 1000 release. If the CallPilot Network Message Service (NMS) feature package is required on CS 1000, please ensure package #175 (NMS) is enabled. The following outlines the various releases and associated software service bundles needed.

CS 1000 Rls 4.0 – Network Message Service option (175) requires Advanced Network Services (L3B)
CS 1000 Rls 4.5 – Network Message Service option (175) requires Advanced Network Services (L3B)
CS 1000 Rls 5.0 – Network Message Service option (175) requires Premium Services (T2)
CS 1000 Rls 5.5 – Network Message Service option (175) requires Premium Services (T2)
CS 1000 Rls 6.0 – Network Message Service option (175) requires Premium Services (T2)
CS 1000 Rls 7.0 – Network Message Service option (175) requires Enhanced Services (T1)
CS 1000 Rls 7.5 – Network Message Service option (175) requires Enhanced Services (T1)

4.4 X21 PEPs to support CallPilot 5.1

It is highly recommended to review the following bulletins located at: https://support.avaya.com/espl for supplemental PEPs that might be applicable.

- X21 Release 3.0 (and later) and DepList Integration Bulletin – CallPilot
- X11 Release 3.0 (and later) and DepList Integration Bulletin – CallPilot/SCCS Integration

4.5 X21 CS 1000– PEP MPLR28776 for CLID/Call Sender issue

CS 1000 R5.0 sends phone number of caller, but R5.5 sends CDN of CallPilot due to interaction with A03/A06 on set. Refer to CR # Q02021470.

Workaround: Apply CS 1000 R5.5 or R6.0 PEP MPLR28776.

5 CallPilot software

5.1 CallPilot CD suite

The table below identifies the CDs contained in the CallPilot 5.0 Software packages. Ensure you have the full set of CDs prior to performing any maintenance activity such as re-install, or upgrading from a prior release. CallPilot 5.1 software will be delivered exclusively from the web as a downloadable update.

PEC	CPC	Label	Version	Date	Notes
NTUB50MA	N0102464	201i Platform 5.0 Image (3 CD set)	05.00.41.20	16-Jan-07	1
NTUB50TA	N0169569	202i Platform 5.5 Image (1 DVD set)	05.00.41.20	09-Oct-08	1, 3
NTUB50NA	N0119717	703t Platform 5.0 Image (3 CD set)	05.00.41.20	16-Jan-07	1
NTUB50PA	N0119718	1002rp Platform 5.0 Image (3 CD set)	05.00.41.20	29-Oct-07	1
NTUB50QA	N0119719	1002rp T1 Platform 5.0 Image (4 CD s	05.00.41.20	22-May-07	1
NTUB50SA	N0119714	600r Platform 5.0 Image (1 DVD set)	05.00.41.20	16-Jan-07	1
NTUB50RA	N0119713	1005r Platform 5.0 Image (1 DVD set)	05.00.41.20	16-Jan-07	1
NTUB50UA	N0215435	1006r Platform 5.0 Image (1 DVD set)	05.00.41.20	22-Apr-10	
NTUB40KA	N0119704	5.0 Applications CD	05.00.41.20	22-Mar-07	3
NTUB43CA	N0119711	5.0 PEP	05.00.41.xx		4
NTUB41FA	N0200929	Unified Messaging Software CD	05.00.41.67	10-Dec-08	5
NTUB44KA	N0200930	5.x Language Prompts – CD 1 of 2	05.00.43.00	10-Dec-08	2
NTUB44KA	N0200930	5.x Language Prompts – CD 2 of 2	05.00.44.00	10-Dec-08	2

Notes:

1. Which platform-image CDs are shipped, NTUB50MA, NTUB50NA, NTUB50PA, NTUB50QA, NTUB50SA or NTUB50RA depends on which platform was ordered.
2. Previously delivered as three (3) CDs, these have now been merged into a two (2) CD set.
    a. Updated language CDs will be made available periodically as language localization expands. Refer to the Language Availability table for details.
    b. CallPilot 5.0 language CDs are applicable to CallPilot 5.1 but are **NOT** interchangeable for use with 1.x, 2.x, 3.0, or 4.0 servers.
3. 202i IPE platform requires use of the revised Applications CD (dated 08-Oct-2008)
4. The PEP CD has been discontinued. Reference ESPL for latest updates.
5. The Unified Messaging Software CD contains both the Desktop Messaging software CD (NTUB41EA) and My CallPilot Software/Updates CD (NTUB48CA), obsolescing individual CDs.

5.2 Default Passwords

CallPilot servers are shipped from the factory with the Windows Server 2003 Operating System and CallPilot application software pre-installed with the default passwords listed below. These default passwords also apply if re-installing CallPilot software via the "Image" CDs.

Description	Account	Default Password
Windows Administrator	Administrator	Bvw250
CallPilot Manager	000000	124578
pcAnywhere	CallPilotDist	%d</\>Ra.Cp5

Notes:

1. When logging into an account, or running Configuration Wizard for the first time, you must change the passwords.
2. Strong passwords have been enabled for Windows Server 2003 Administrator account. When you change this password using Configuration Wizard, you can no longer use simple passwords. As with all accounts, it is highly recommended that strong passwords be utilized.
3. CallPilot has strong passwords configured to contain a minimum of 6 characters plus at least 3 of the following; uppercase, lowercase, symbols and numerals.
   For example *p2leO4>F.
4. The OS password can be changed without rebooting the server via running Configuration Wizard and once changed, canceling out before completing the procedure; or by simply using Ctrl-Alt-Delete and selecting the "Change Password" option on the pop-up window.
5. There is no utility available to recover the Windows Server 2003 administrator account password. Carefully guard this password as re-imaging is the only option to recover the system.

6 Feature Information & Limitations

6.1 Language Availability

At the time of this printing, CallPilot 5.0/5.1 provides support for the following languages.

Previously, these were released on three (3) separate region-specific CDs, but at the time of this printing, have been condensed and are only provided on two (2).

Language	Voice Prompts Language File Number	Original CD	Revised CD
Arabic	Lang1025	EMEA (05.00.44.00)	CD 2 of 2
Cantonese	Lang3076	Asia/Pacific (05.00.43.00)	CD 1 of 2
Catalan	Lang1027	EMEA (05.00.44.00)	CD 2 of 2
Czech	Lang1029	EMEA (05.00.44.00)	CD 2 of 2
Danish	Lang6	EMEA (05.00.44.00)	CD 2 of 2
Dutch (Standard)	Lang1043	EMEA (05.00.44.00)	CD 2 of 2
English, American (US)	Lang1033	Americas (05.00.43.00)	CD 1 of 2
English, Australian	Lang3081	Asia/Pacific (05.00.43.00)	CD 1 of 2
English, Canadian	Lang4105	Americas (05.00.43.00)	CD 1 of 2
English, Irish	Lang6153	EMEA (05.00.44.00)	CD 2 of 2
English, UK (female)	Lang2057	EMEA (05.00.44.00)	CD 2 of 2
Finnish	Lang11	EMEA (05.00.44.00)	CD 2 of 2
French, Canadian	Lang3084	Americas (05.00.43.00)	CD 1 of 2
French, European	Lang1036	EMEA (05.00.44.00)	CD 2 of 2
German	Lang1031	EMEA (05.00.44.00)	CD 2 of 2
Greek	Lang1032	EMEA (05.00.44.00)	CD 2 of 2
Hebrew	Lang1037	EMEA (05.00.44.00)	CD 2 of 2
Hungarian	Lang1038	EMEA (05.00.44.00)	CD 2 of 2
Italian	Lang1040	EMEA (05.00.44.00)	CD 2 of 2
Japanese	Lang17	Asia/Pacific (05.00.43.00)	CD 1 of 2
Korean	Lang1042	Asia/Pacific (05.00.43.00)	CD 1 of 2
Mandarin, PRC	Lang2052	Asia/Pacific (05.00.43.00)	CD 1 of 2
Mandarin, Taiwanese	Lang1028	Asia/Pacific (05.00.43.00)	CD 1 of 2
Norwegian	Lang1044	EMEA (05.00.44.00)	CD 2 of 2
Polish	Lang1045	EMEA (05.00.44.00)	CD 2 of 2
Portuguese	Lang2070	EMEA (05.00.44.00)	CD 2 of 2
Portuguese, Brazilian	Lang1046	Americas (05.00.43.00)	CD 1 of 2
Russian	Lang25	EMEA (05.00.44.00)	CD 2 of 2
Slovak	Lang1051	EMEA (05.00.44.00)	CD 2 of 2
Spanish, Castilian	Lang1034	EMEA (05.00.44.00)	CD 2 of 2
Spanish, Latin American	Lang3082	Americas (05.00.43.00)	CD 1 of 2
Swedish	Lang29	EMEA (05.00.44.00)	CD 2 of 2
Thai	Lang1054	Asia/Pacific (05.00.43.00)	CD 1 of 2
Turkish	Lang1055	EMEA (05.00.44.00)	CD 2 of 2

6.2 Meridian Mail Migration

Migration from Meridian Mail systems to CallPilot 5.1 is supported using the Meridian Mail migration utility tape NTUB25AC (available within NTUB24BC Migration Package). This supports migration from all Meridian Mail MM11, MM12, and MM13 releases for all Meridian Mail platforms **except the MSM and Card Option running MM13.11.2**. It is required for all Meridian Mail releases including MM13.14 as this tape supersedes the migration utility available in the TOOLS level.

Notes:

1. Previous versions of the migration utility NTUB24AA, NTUB24AB, NTUB24AC cannot be used with CallPilot 5.1. The Migration guide should be consulted for limitations.
2. It is highly recommended the latest Meridian Mail to CallPilot Migration Utility Guide, Release 5.1 documentation be referenced when performing a migration. Check the Avaya Partner Portal website for the latest version of this document. At the time of this printing, the latest version is NTP NN44200-502: *Meridian Mail to CallPilot Migration Utility Guide* Release 5.1, Standard 01.06.
3. The Mailbox Number is a unique identifier on both the Meridian Mail and CallPilot voice mail systems. If the migration utility encounters a CallPilot mailbox with the same number as a Meridian Mail mailbox, then the utility will overwrite the existing mailbox in order to avoid a duplicate.
4. CallPilot requires use of the NTRB18CAE5 (DS30) or NTRB18DxE5 (CAT-5E) MGate card for connectivity. Systems migrated from Meridian Mail EC11 must use only the updated MGate cards are used.
5. When migrating from Mail to CallPilot, it is recommended to remove any RPLs defined in CallPilot first and then migrate the Mail mailbox/message and system data over.

6.3 Upgrade and Setup Wizards

Security enhancements:
As of CallPilot 5.0, the Challenge Response Authentication option for IMAP or SMTP is no longer supported. The Upgrade Wizard notifies/warns, before doing the backup that these options are selected and will no longer be supported. However, the craftsman may not change anything so it is desired to warn them again during the Setup Wizard that the option is still set but will not be used. This is done after the restore but before the data base upgrade

6.4 Installation & Upgrades

- **MyCallPilot 05.xx:** The client cannot be loaded onto a standalone server running release 2.5 of CallPilot Manager. Recommendation – Upgrade CallPilot Manager/Reporter to 5.1.
- **Image CDs:** Using the wrong image CD on a server (i.e. 201i on a 1002rp) will cause unpredictable results i.e. the image will install but the system will not work correctly. The Upgrade Wizard will check that you have the correct CDs.
- **Directory sync feature**: CallPilot will add a directory sync admin mailbox. If your system has maxed out the number of users allowed by your keycode it will fail to add the dirsync admin mailbox. Before upgrading your system, you should free up one (1) mailbox or request a keycode with additional mailboxes

- **NTRB18DxE5 CAT-5E MGate cards:** When using CAT-5E connectivity (NTRH40CAE5 MPB96 board and NTRB18DxE5 CAT-5E MGate cards), if the MGate cards will be populated in separate CS 1000 media gateways, ensure that two gateways are clock synchronized using NTDW67AAE6 / MGC Clock Reference Cable. When using Option-11C cabinets with the clocking cable, the NTDW63AAE5 / MGC Breakout Adapter for Option 11C are also required. A clock source (such as PRI card) is required in one of the media gateways or both media gateways if the synchronization cable is not used.

  Reference support bulletin 025223-01 for additional details.

6.5 Drivers/Firmware

WARNING: Do not use the Windows Device Manager to update or uninstall the MPB16 or MPB96 drivers. The device manager will not configure the drivers correctly, resulting in a blue screen. The drivers come pre-installed on the CallPilot server and are re-installed when the CallPilot server software is re-installed either via re-imaging or the Applications CD.

- PEP CPDRVPEP001S introduces the support for the US Robotics USR5637 56K USB Faxmodem on 202i, 600r, 1005r, and 1006r platforms.
- PEP CPDRVPEP002S introduces the support for the USB RDX External Hard drive on 202i, 600r, 1005r, and 1006r platforms.

6.6 Backup/Archive/Restore

- CallPilot 5.1 and later archives/backups are not compatible with earlier versions due to supplemental changes within the database. After completing the upgrade to CallPilot 5.1, it is recommended to perform a new full-system backup and/or user archive.
- It is recommended that after the CallPilot system is brought in-service, a new full-system backup and/or user archive is performed.
- Restored customized prompts from CallPilot releases 2.02 or 2.5 to CallPilot 5.1 are only supported if the customized archive is performed with CallPilot 2.02 with SU3 or later or CallPilot 2.5 with SU1 or later.
- Backup to an externally connected HDD is supported on 202i, 600r, 1005r, and 1006r platforms. It is required to install PEP CPDRVPEP002S. PEP CPDRVPEP002S introduces the support for the USB RDX External Hard drive.

6.7 CallPilot Manager

- The CallPilot Manager software provided with CallPilot 5.1 can be used to administer CallPilot servers running releases 3.0, 4.0, and 5.0. Support for 2.5 servers is no longer available due to Daylight Savings Time updates which aren't available for 2.5 (Windows NT 4.0 Server-based) systems.
- CallPilot 5.1 uses the strong password option on Windows Server 2003 for the administrator account. When you change the password using Config Wizard you can no longer use simple passwords. For a strong password, you must comply with three (3) of the following rules:
  - A lower case character
  - An upper case character
  - A number
  - A special character (punctuation)
- Do not set the Windows Server 2003 security policy "Minimum Password Age" to anything but a value of 0. This will force you to change your passwords every day. Setting this value to one (1) could result in the config wizard failing when it attempts to update the password.
- If you have a Citrix client installed on your standalone web server, you must install My CallPilot and Reporter using the Add/Remove option of Windows. This is a Citrix requirement.
- Web client browsers can only view CallPilot on-line help if a Java Runtime Environment (JRE) is installed on the client PC. Microsoft no longer distributes their own JRE in Windows products. CallPilot 5.1 has been tested with JRE versions 1.4.2 and 1.5(5.0). JRE Version 1.4.2 is included on the Application CD and both are downloadable from the following site: http://www.oracle.com
- Firefox browser cannot be used to play/record greetings or personal verifications from CallPilot Manager. It gives you a "not supported" type of message which is incorrect.
- CallPilot Manager does not display the "Application Builder" link if a browser other than Internet Explorer is used, even if AppBuilder is installed on the customer-provided web-server.

6.8 High Availability

- High Availability is only supported on the 1005r and 1006r platforms.
- High Availability is supported with Contact Center CCMS 6.x and 7.x integration through supplemental PEPs. Changes to the CS 1000, CallPilot, and Contact Center were required to introduce this functionality. These changes are detailed in the below section 'Contact Center Interoperability'.
- A configuration video is available for download from the Support Portal webpage. This self-paced tutorial covers installation and configuration of a CallPilot High Availability system, plus describes other High Availability concepts and terminology.
- The instructional video can be located on the CallPilot page, under the Downloads sub-heading. A direct link to the configuration video is available at:
  https://support.avaya.com/css/SAFE/downloads?downloadId=9459
- The Contact Center/Symposium Integration is not covered in this video. For integration details, please refer to the Feature Information & Limitations/Contact Center Interoperability section of this document.

- A High Availability (with Contact Center integration) training webinar is also available. Reference course #6350W for details. Contact Messaging Product Management (brassard@avaya.com) for access to this.

6.9 My CallPilot and Desktop Messaging

6.9.1 MWI Icon in system tray

- In order to receive full functionality, the MWI icon must be connected to a CallPilot 5.x server. If logged into a 4.0 or earlier server, only partial functionality will be provided.

6.9.2 Features that require a 5.1 server (Backward compatibility limitations)

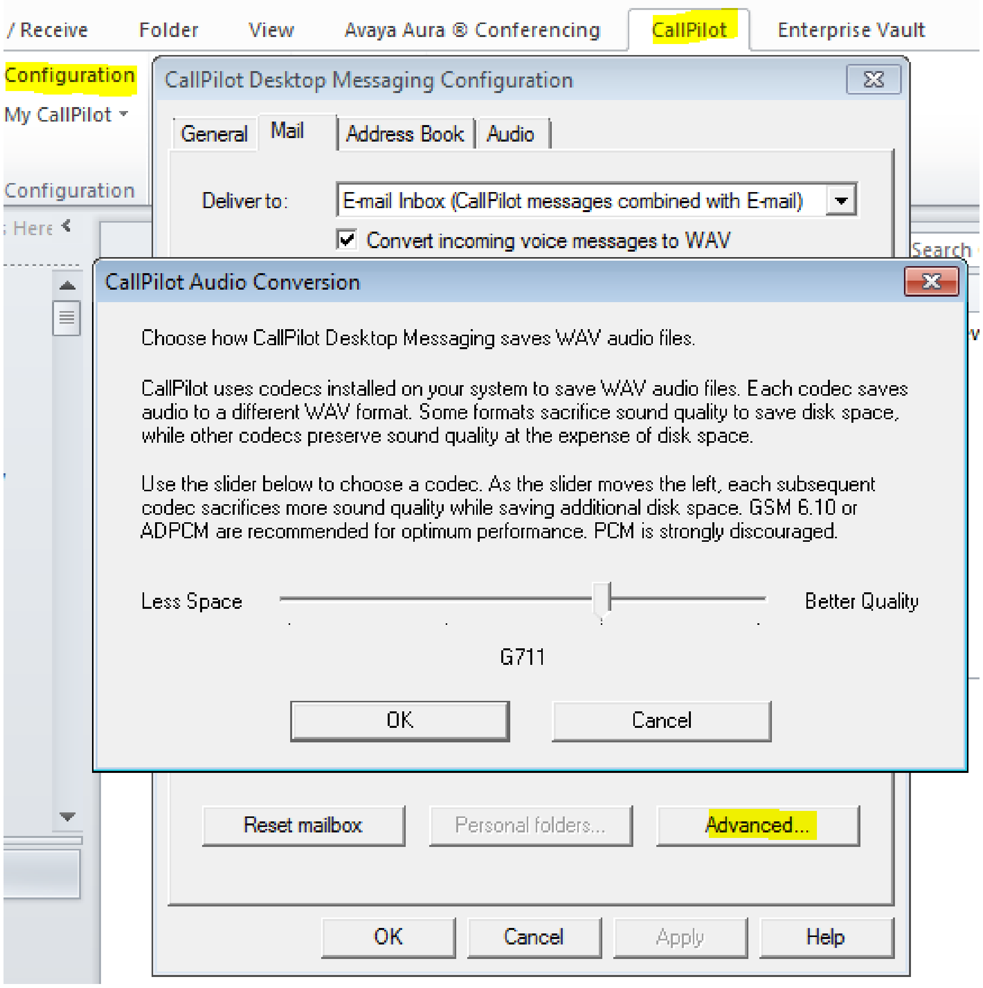
- The following features require a 5.1 CallPilot Server:
    - Update Existing Outlook Contacts
    - Download of CallPilot address book (desktop messaging)
    - New Check Names Capability
    - Spell Checker, Mark Messages as unread
    - My CallPilot URL Update
    - Ping on Startup, Text Capability COS
    - Access to Lotus Notes Public Address Book COS
    - Printing Desktop Client COS settings
    - Desktop Link to Greetings
    - Desktop Link to Configure MFR
    - Geographic Redundancy (requires both servers in pair be on same release, preferably 5.1 but back to 5.0/SU09; desktop client 5.00.41.141 or later; and My CallPilot 5.00.41.141 or later hosted from a customer-provided web-server).

6.9.3 Desktop Messaging / Outlook Message Store

- The first time that CallPilot 5.1 desktop is installed and run on a client desktop running Microsoft Outlook, the user will be presented with the option to select their message store in Outlook. The options presented are a separate CallPilot messaging store folder or the Outlook email message store folder. If Outlook email message store is selected, the CallPilot message store folder is displayed in Outlook even though the email folder was selected. Messages are not directed to this CallPilot. To remove the CallPilot message store folder from Outlook, exit and re-run Outlook and the CallPilot message store folder will not be displayed.
    - This procedure only needs to be executed once. Future execution of the desktop client will not have the CallPilot message store folder visible. This behavior is a Microsoft Outlook limitation.

6.9.4 Desktop Messaging / WAV encoding format setting

- Desktop Messaging includes a hidden feature that allows the user to change the WAV encoding format (GSM 6.10, ADPCM, G.711, or PCM), balancing audio quality, LAN friendliness, storage requirements, and expanding compatibility with various devices.
    - From the email client toolbar, select "CallPilot", then "Configuration", then the "Mail" tab.
    - While holding down CTRL-Shift keys, press the "Advanced" button.
    - Use the slider to pick the encoding format of choice.
    - Click "OK" to close the pop-up window.
    - Click "Apply" to save the changes; or "OK" to save the changes and exit configuration.
    - The changes will be active when the groupware client is restarted.



Deliver to: E-mail Inbox (CallPilot messages combined with E-mail)

☑ Convert incoming voice messages to WAV

Choose how CallPilot Desktop Messaging saves WAV audio files.

CallPilot uses codecs installed on your system to save WAV audio files. Each codec saves audio to a different WAV format. Some formats sacrifice sound quality to save disk space, while other codecs preserve sound quality at the expense of disk space.

Use the slider below to choose a codec. As the slider moves the left, each subsequent codec sacrifices more sound quality while saving additional disk space. GSM 6.10 or ADPCM are recommended for optimum performance. PCM is strongly discouraged.

G711

6.9.5 My CallPilot / Browser Support

- **Firefox Browser support on Windows**
    - My CallPilot 5.x supports the Firefox browser on the Windows OS. The embedded CallPilot audio player will not be available in this browser
- **Safari Browser support on Mac OS X**
    - No CallPilot fax driver or CallPilot Audio Player is provided. Users can use the QuickTime Player to listen to WAV audio attachments
- **Mozilla Browser support on Linux**
    - No CallPilot fax driver or CallPilot Audio Player is provided. Users can use the QuickTime Player to listen to WAV audio attachments
- **Microsoft Internet Explorer 9 and 10**
    - Requires "Compatibility View" be turned on. Use the following steps:
        - Launch Internet Explorer 9
        - Within the "Address" bar, click the "Compatibility View" button
- Windows 8 (x64 Edition)
    - Requires 32-bit "CallPilot Player" is installed

6.9.6 My CallPilot / Windows 2008 x64 bit compatibility

- In order to run 32-bit web applications on Windows Server 2008 x64-bit, you should manually enable 32-bit applications (My CallPilot) using the IIS Manager Utility. To do this, perform the following steps:
    1. Log into your customer-provided web-server
    2. Open IIS Manager by clicking your Windows Start button and entering "inetmgr" into the search box and pressing <Enter>.
    3. On the Connections pane, expand the server node and click "Application Pools".
    4. Right click on "DefaultAppPool" and select "Advanced Settings…"
    5. Change "Enable 32-bit Application" to True.
    6. Click "OK" to finish.

6.9.7 My CallPilot and Desktop / Callback DN used for Call Sender

My CallPilot and Desktop use mailbox callback DN for the Call Sender feature. If this field is blank, then a blank DN will be presented to the user. The user can simply enter the extension DN to call the user.

Note: This only needs to be done once. My CallPilot and Desktop will remember what is entered and use it in the future.

6.9.8 Outlook

- Adding / Updating recipients to contact list fails to update recipient in original message under the following condition:
    - CallPilot Message resides in MS Outlook Exchange Inbox
    - User is running MS Outlook 2002 / XP

  (This is likely a bug with MS Outlook as MS Outlook 2003 works properly)

6.9.9 GroupWise

- GroupWise 7.0 (3/30/2006) client release does not support the CallPilot address book from CallPilot Desktop client. Novell confirmed that this is a GroupWise client problem and it was fixed in GroupWise 7.01. Development has confirmed that this issue is indeed fixed in the GroupWise 7.01 release.

6.9.10 Conversion from Outlook to GroupWise

- Under certain conditions, desktop messaging may fail to launch after conversion from Microsoft Outlook to Novell GroupWise. This is due to the default mail profile stored in the Windows registry not being removed/updated properly after uninstalling Outlook. When GroupWise is installed, it creates its own profile, but is not the default profile, which has negative impacts on CallPilot desktop messaging operation. Refer to wi01175933.

Steps performed to reproduce scenario:
a) Have Windows 7 with Outlook 2013 installed
b) Uninstall Outlook 2013
c) Install GroupWise 2012/Service Pack 1
d) Install CallPilot Desktop Messaging
e) Launch GroupWise and encounter a crash

Workaround:
a) Have the system with GroupWise 2012 and legacy Outlook's profile.
b) Download 'MFCMAPI 32 bit executable' tool from: http://mfcmapi.codeplex.com/ 'Download' section
c) Launch it on the PC. Choose 'Profile' menu and then 'Show Profiles'
d) In the 'Profiles' dialog, right click on the correct profile ('Novell GroupWise') and then click 'Set default profile'
e) After that install DM and it should work without problems

6.9.11 CPWipe Enhancement (For desktop only)

If Desktop installation is used under multiple user accounts on a single PC every one of them will have user-specific Desktop settings saved within their accounts. During Desktop un-installation those setting will be removed only from user who installed Desktop in the first place, leaving all other users unchanged. This is standard behavior which allows seamless re-enabling of Desktop in case of later installation on the same PC. If this is considered as some sort of security flaw, administrator can use a special "CPWipe" utility (distributed with Desktop) to remove user-specific leftovers after Desktop was un-installed from the system. It can be used in two modes: automated and manual.

- Manual mode is pretty straight: login under target user account and launch cpwipe.exe, a pop-up message will appear, asking if you want to remove all setting (press "Yes" to remove). There is a special option which allows silent mode to be enabled for this utility: type "cpwipe.exe –silent" in command line. Using this option it's possible for administrators to run this utility for multiple users with some kind of script.

- Automated CPWipe mode is a complicated one: it was designed primarily not to remove leftovers, but to reset settings for every Desktop user on Desktop re-install/upgrade. It will only be activated when a user logins into system next to Desktop re-install/upgrade, this implying that all sensitive data will not be removed till that time. To enable Automated CPWipe feature administrator must prepare a customized installer (please refer to NTP for more details). In the created 'setup.ini' file you should change CPWIPE_ACTIVE property value to "1". When administrator will installs such a customized installation on a target PC, every user that will use Desktop with Outlook or GroupWise must use "Add CallPilot to Default Mail Profile" shortcut (located in Nortel -> CallPilot Desktop Messaging) before using Desktop for first or there will be no Desktop controls in groupware client. NOTE: Automated CPWipe is re-armed every time Desktop is "upgraded" or "repaired" with a new property enabled (in "setup.ini" file), wiping all users setting on subsequent login. This is not happening in "Modify" mode.

CPWipe limitations:

- CPWipe feature is designed to work with Desktop at least version 5.0. It works during Desktop 5.0 version upgrade to another 5.0 sub-version or 5.1. It does not work during Desktop upgrade from version earlier than 5.0.
- Automated CPWipe feature is relying on MWI Icon component in order to be activated. If MWI Icon shortcut is removed from startup menu then Automated CPWipe feature will not work.
- CPWipe was not designed to remove CallPilot messages from user mailbox; it only removes user-specific settings and files for current user.

6.9.12 My CallPilot Audio Player with Internet Explorer 10

My CallPilot users may experience the issue when CallPilot Audio Player disappears or is not displayed fully in the Internet Explorer 10 browser. This is a result of some changes made to the HTML frames rendering engine within IE10. Refer to wi01104902. This issue is resolved in My CallPilot version 5.01.03.03 and later.

Workarounds:

- Resizing the browser's window often makes the player reappear
- Use previous versions of the IE browser
- Use another compatible browser such as Firefox or Google Chrome

6.10 Shared Telephone/Dorm Room

6.10.1 Limitations

- With dual language prompting, if the Shared DN System Greeting is recorded in both (primary & secondary) languages, the customized greeting is played only in the primary language, and the default "No one is available …." Is played for the 2nd language.
- For users that shared a DN, they cannot use the "#" as the mailbox number during login. The system used to use the calling DN to find the mailbox, but now, there is no way to determine to the mailbox number as there will be more than one (1) mailbox found.
  Workaround: Enter the mailbox number.

6.11 Remote Access

- Avaya has tested with and reports compatibility with the following remote-control applications for use with CallPilot 5.0 systems:
  - Symantec pcAnywhere
  - Microsoft Remote Desktop Connection (RDC)
    - Refer to product bulletin P-2005-0026-Global for details.
  - WebEx
    - Refer to product bulletin P-2007-0062-Global. See "Known Problems" section for issues with co-existence of WebEx and pcAnywhere.
  - LogMeIn Rescue
  - RealVNC 4.1
    - Per wi00677884, last tested version was VNC Free Edition 4.1.3.
- When logged in through Microsoft RDC remote desktop you **must** be connected to the root console to use any CallPilot tools (e.g. installing PEPs, accessing Support Tools, etc.). This requires using "Method-1/Private" (connecting to IP address with "/console" suffix) or if using "Method-2/Shared" by running the 'shadow 0' command after logging in.

  For more information see: Product Bulletin P-2005-0026-Global "CallPilot 3.0 and the 201i IPE Platform – Using Microsoft Remote Desktop Connection".

- When trying to connect to a 201i from a desktop using Microsoft RDC remote desktop, an error may occur which may block connecting to the server. This is a Microsoft problem as outlined in "The RDP protocol component "DATA ENCRYPTION" detected an error in the protocol stream and has disconnected the client "Microsoft Knowledge Base Article – 323497" You can read the solution here: http://support.microsoft.com/?kbid=323497.
- RDC is known to potentially disrupt ELAN communications activity between CallPilot and the switch, causing possible dropped calls or RNA conditions. This is a known issue with Microsoft, without any estimated time of resolution. It's exhibited primarily on lower-bandwidth connections and with lower-CPU capable systems (201i IPE). RDC may still be used for remote maintenance, but is at the customer's own risk.

6.12 Reporter

- If you have a Citrix client installed on your standalone web server, you must install My CallPilot and Reporter using the Add/Remove option of Windows. This is a Citrix requirement.

- Reporter has a limitation when selecting start and end times to generate reports. The report start time should be on the full hour but the end time is not critical, as long as it is after the end of the time period that the report is requested. If the start time is not on the full hour (i.e. 1:00, 11:00), any events that occur from the start time to the next full hour will be missed. This is a legacy issue and also occurs in previous versions of CallPilot.

  Example 1: assume you want to report on events from 2:02pm to 3:45pm. Any events occurring between these 2 times will not be reported in your report(s). To successfully report between these 2 times, you must enter 2:00pm to 3:45pm.

  Example 2: assume that you want to report on events from 12:15pm to 3:25pm. Any events occurring between 12:15pm and 1:00pm will be missed. Any events occurring from 1:00pm and 3:25pm will be displayed.

- CallPilot 5.x has introduced a Reporter Database Backup tool. This tool is a standalone tool that is installed with Reporter that allows customers to backup their Reporter yellow database. Due to CallPilot's architecture of operational measurements (OM) capture and Reporter, there are some rules and constraints around restoring this backup data.

  The backup tool may be used at any time to perform a backup. Transactions may still be active on the database (i.e. pegging from CallPilot) and a backup initiated. The limitations are with respect to restoring your data. The key to what is supported is that restoration of the data must be completed before logging into the Reporter system. When you restore your data, vital connection information to the CallPilot servers is also restored and then re-used upon login. If you login and then restore your data, the restore brings back the old login information to the CallPilot server, while the CallPilot server now has new login information, and the systems will not allow any pegging of OM data or reporting.

  To further clarify the supported procedures, the following tested scenarios have been included;

  1. Restore after system is recovered without a logout and erase having been performed and no login performed prior to restore.
     a. Perform backup
     b. Uninstall reporter and ensure yellow database is not present on system
     c. Install reporter (**Do not log in to system**)
     d. Restore data
     e. Log in and connect to system
     f. Ensure connection is established
     g. Run a report to ensure restored data is available

2. Restore after system is recovered with a logout and erase having been performed after backup and no login performed prior to restore.
    a. Perform backup
    b. Perform logout and erase
    c. Uninstall reporter and ensure yellow database is not present on system
    d. Install reporter (**Do not log in to system**)
    e. Restore data
    f. Log in and connect to system
    g. Ensure connection is established
    h. Run a report to ensure restored data is available

3. Restore without system recovery without logout and erase having been performed after backup.
    a. Perform backup
    b. Restore data
    c. Log in and connect to system
    d. Ensure connection is established
    e. Run a report to ensure restored data is available

4. Restore without system recovery with logout and erase having been performed after backup.
    a. Perform backup
    b. Perform logout and erase
    c. Restore data
    d. Log in and connect to system
    e. Ensure connection is established
    f. Run a report to ensure restored data is available

Included below are **unsupported** scenarios of restoring Reporter data from the yellow database. These procedures will **not** successfully restore your data and will leave your system without any OM data. These are listed for customers to better understand these described limitations.

1. Restore after system is recovered without a logout and erase having been performed and login is performed prior to restore.
    a. Perform backup
    b. Uninstall reporter and ensure yellow database is not present on system
    c. Install reporter
    d. Log in to system to create new system id
    e. Restore data
    f. Log in and connect to system
    g. Ensure connection is established
    h. The data will not be available

2. Restore after system is recovered with a logout and erase having been performed after backup and login is performed prior to restore.
    a. Perform backup
    b. Perform logout and erase
    c. Uninstall reporter and ensure yellow database is not present on system
    d. Install reporter
    e. Log in to system to create new system id
    f. Restore data
    g. Log in and connect to system
    h. Ensure connection is established
    i. The data will not be available

- If you upgrade your Reporter software to a later version, then you must create a new backup of your Reporter data. Changes to the database architecture may have occurred in the new version of the software, which may render your previous backup inoperable.

- Do not use a Reporter backup created on a previous version of the Reporter software. Changes to the database architecture may have occurred in the new version of the software, which may render your previous backup inoperable.

- Windows Server 2003 web-servers require installation of .NET Framework 2.0 prior to installation of CallPilot Manager/Reporter.

6.13 Message Forwarding Rules

6.13.1 Mark Original Message as Read when Opened by Recipient:

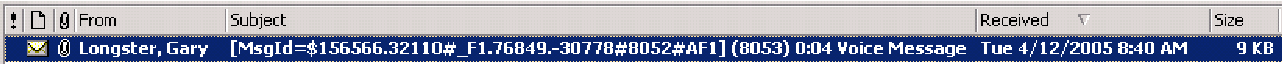
- The feature makes use of the Read Receipt capability of the e-mail server the message was forwarded to. With this option enabled, a Read Receipt will be requested to be returned to the CallPilot system when the forwarded message is Read. CallPilot will recognize the returned Read Receipt when either:

1. A MIME message with "Content-Type: multipart/report; report-type=disposition-notification" is received, AND, an "In-Reply-To:" or "References:" field is found containing the Message ID of the original message,

-Or-

2. A MIME message with "Content-Type: text/plain" is received, AND, a subject field is found containing the string:

"[MsgId="the Message ID of the original message, and the string "]". For example:



!	🗋	0	From	Subject	Received ▽	Size
	✉	0	Longster, Gary	[MsgId=$156566.32110#_F1.76849.-30778#8052#AF1] (8053) 0:04 Voice Message	Tue 4/12/2005 8:40 AM	9 KB

If CallPilot is able to extract the Message ID from an incoming Read Receipt, CallPilot will mark the message with that Message ID as Read. If this was the only message in the user's mailbox that was Unread, the MWI light on the user's phone will be turned off. If the message had already been marked Read then no action will be taken.

Not all e-mail servers support Read Receipts. For example, at the time the document was written, Yahoo Mail and other popular e-mail servers did not support Read Receipts. It is up to the user to determine if their e-mail system supports Read Receipts.

To determine if the user's e-mail server supports Read Receipts, follow these steps:

1. Configure a CallPilot mailbox to forward to an account on the desired email server.
2. Send a message to that mailbox. Verify that the MWI goes on at the corresponding phone (MWI DN).
3. Verify that the message is received at the email account. (If possible, verify that a Read Receipt is requested.)
4. Read the message. (If possible, verify that a Read Receipt is sent out.)
5. Verify that the MWI light goes out on the phone (may have to wait a minute or so).

   If the MWI goes out, this email server currently supports Read Receipts.

Also, some systems give Read Receipts a lower priority than other messages, and Read Receipts may not be returned to the CallPilot system immediately.

This Read Receipt feature is not supported when forwarding messages to a CallPilot mailbox. The option is disabled if a CallPilot mailbox address is selected as the forwarding target.

6.13.2 Troubleshooting

The administrator can troubleshoot this feature by asking the user to check her CallPilot mailbox for Read Receipts from the external e-mail server. If a Message ID is not found, the message is treated as a normal Read Receipt and deposited into the user's mailbox (without error). If the feature is working properly, there will be no Read Receipts deposited into the user's mailbox because Read Receipts are deleted when the associated message is marked as Read.

If the event **54865 parsing error** is present in the Event log, a valid Read Receipt was received but a corresponding CallPilot message was not found. This is because the message had already been deleted.

The Event Log can be accessed in 2 manners:

1. The Windows Start button → Programs → Administrative Tools → Event Viewer
2. CallPilot Manager: System tab → Event Browser

If Read Receipts are not reliably returned or do not contain the information required to match them with the originally forwarded message, then the Message Forwarding Rule should be configured to either Mark the message as being Read when the message is forwarded or uncheck the 'Mark original message as Read' checkbox.

6.14 Remote Notification

6.14.1 Customized Remote Text Notification (RTN) limit

- CallPilot 5.1 introduced customizable remote-text notification capability, configured either by the system administrator (via CallPilot Manager) or end-user (via My CallPilot). The notification message field is limited to 128 characters. Refer to wi00986307.

6.14.2 Remote Notification (RTN) setup display in IE

- Using My CallPilot 05.01.01.07 with Internet Explorer 6.0 and 7.0, two fields “Email address” and “Notification Messages” are not aligned properly in Notification Target Setup page. This is due to limitations within IE6 and IE7 not displaying HTML strings properly. This issue is limited to IE6 and IE7. Refer to wi01027289.

Workaround: Use more recent versions of Internet Explorer (IE 8, IE9 or IE10) or another browser.

6.14.3 Remote Notification – multiple targets and Event 58704

- A user may configure multiple Remote Notification telephone target DNs in mailbox properties through CallPilot Manager. When the user logs into their mailbox from the TUI and tries to update the first RN telephone target DN, having entered a notification number that already exists in the list of RN target DNs configured for this mailbox, CallPilot does not update the first RN target DN with the notification number and logs SLEE event 58704 “Error updating profile data. Object Module rc=60873”. Additionally, CallPilot does not play any prompts to the user in order to notify that the RN target number is not updated. Refer to wi01055954 and wi01027289.

  LDAP return code 60873 means that CallPilot cannot update a record of the first RN target because another record with the same target DN already exists in the database.

  When RN target is not updated via the TUI, CallPilot does not play any prompts because appropriate prompts have not been recorded for Multiple Remote Notification feature. MRNT feature was developed without support of the Telephone User Interface.

6.15 Geographic Redundancy

6.15.1 CallPilot GR with Contact Center Integration – No Automatic Failover for voice services (IVR and ACCESS)

- CallPilot and Contact Center integration require communications between applications themselves as well as the switch, utilizing both the ELAN and CLAN. Both CallPilot and Contact Center are configured with a single static IP address of the other application. Additionally, Contact Center is configured to acquire CallPilot "resources" (channels) to use when scripted call processing events occur.

  When a CallPilot that is providing voice services for Contact Center being taken offline or fails, there is no automatic failover of those voice services as Contact Center doesn't know of the "paired" system's IP address or resources.

  If both CallPilot servers within a GR pair and the Contact Center Management server are on the same switch, if the "active" system is taken offline, manual intervention is required within the CCMS server to transition to the second CallPilot server and its resources.

  Refer to Appendix-G for additional details on GR failover scenarios.

6.15.2 CallPilot GR with My CallPilot

- My CallPilot version 5.01.01.07 (or later) offer automatic failover from system-X to system-Y for users of the service, but only when My CallPilot is installed on a customer-provided web-server.

6.15.3 CallPilot GR and Desktop Messaging

- CallPilot GR requires use of Desktop Messaging client 5.01.01.07 (or later) for automatic failover of desktop messaging functionality. If earlier versions of the client are used when GR is configured, no failover of desktop messaging will occur if the primary system is offline.

6.15.4 High Availability and Geographic Redundancy are mutually exclusive.

- CallPilot servers with the High Availability feature (paired 1005r or 1006r servers with EMC AutoStart software) cannot also apply Geographic Redundancy. Only one "resiliency" feature is permitted at any given time.

6.15.5 User Restore can fail after running GR rebuild

- An administrator may receive errors on restoring users from user-archive after running GR Rebuild procedure on the same server. Refer to wi00833774.

  Workaround: Administrator should delete existing users prior to restoring from archive.

6.15.6 GR and system administration

- For CallPilot servers with the Geographic Redundancy feature enabled, it's important to ensure that when database changes occur which directly affect mailboxes on one system, they also occur on the GR partner server. For example, if a new Mailbox Class, Shared Distribution List, or Restriction/Permission List is added to one server, it should also be added to the GR partner server so that synchronization can occur properly. Refer to wi00844148 and wi00888922.
- If unsure, use the "GR Comparison Diagnostic" which will simplify identification of inconsistencies in the settings within CallPilot that could negatively impact GR synchronization.

6.15.7 GR and RN – potential data loss

- If upgrading from CP5.0 SU07 a potential problem has been identified that, if experienced may result in a situation where all Remote Notification targets are lost after upgrading to a future Service Update (e.g. SU11) or release (e.g. CallPilot 5.1). If this issue has already occurred then nothing can be done and all Remote Notification targets must be input manually. If not already upgraded, please avoid manual uninstallation of CP5.0 SU07 suite of PEPs. Instead please always launch the future Service Update installer so that SU07 and corresponding PEPs are removed automatically. Refer to wi00838251.

6.15.8 GR and CallPilot "Busy Line" notification

- Due to a limitation in the way a caller is forwarded to the second CallPilot server when the first CallPilot server's CDN is in default mode, the initial CallPilot prompt may not be accurate if the user's mailbox has the "Callers notified of busy line" checkbox enabled.

  In this scenario, the caller will always hear the prompt "The person at extension XXXX is on the phone" prior to the user's greeting even though the user may not be on the phone at the time of the call. Refer to wi00963447.

6.15.9 GR does not sync users who are Temporary Remote Users on partner

- CallPilot Geographic Redundancy (GR) does not synchronize users if the same users are present on the GR partner as "Temporary Remote Users" (TRUs). Refer to wi00978929.

  Workaround: To resync users, administrator deletes existing TRUs from the GR partner.

6.15.10 GR and use of Survivable Media Gateways (SMGs)

- CallPilot GR can be implemented with one of the servers located in a Survivable Media Gateway (SMG); however this is not a desired or recommended implementation.
- In a "rainy day" mode involving failure of the primary CS 1000 core, the once active CallPilot system will automatically fail over to the CallPilot located in the Survivable Media Gateway (SMG). However, the SMG-based CallPilot will remain offline until administration is performed. This is due to the SMG becoming the active core and offering a new ELAN IP address to all installed applications (CallPilot, Contact Center, etc.). To restore voice messaging, auto-attendant, and other functions, the CallPilot server must be re-configured to the new SMG ELAN IP address using the CallPilot Configuration Wizard utility.

6.15.11 GR cannot replicate if notification message contains CR/LF

- CallPilot GR synchronization fails to replicate messages if users have optional “Notification Message” text configured with carriage-return and line-feed (two lines). Refer to wi01186246.

  Workaround: In My CallPilot, CallPilot Features, Message Notification, when “Notification Device” equals e-mail, ensure “Notification Message (optional)” does not include carriage return (ASCII-13) and line-feed (ASCII-10). If more than one line is desired, continue typing text and allow it to wrap rather than using CR/LF.

7 Procedures

This section describes any key steps or last minute changes to the upgrade procedure for CallPilot 5.0. To ensure a smooth upgrade to CallPilot, it is imperative that you review all of the information contained in this section.

7.1 Upgrade Guide

Before upgrading your system, make sure that you have the latest copy of the Upgrade Guide NTP, available for download from the Avaya Partner and/or Support Portal websites. Use the following direct link to the CallPilot page:

https://support.avaya.com/products/P0712/avaya-callpilot/

7.2 Upgrade Wizard

When upgrading a system from 5.0 to 5.1, you must run the Upgrade Wizard on your current system to ensure that your current hardware and data is valid to upgrade to CallPilot 5.1. *Failure to run the upgrade wizard may result in a failure in the upgrade process or an unstable system.*

Retrieve the latest Upgrade Wizard from the Enterprise Solutions PEP Library (ESPL) using PEP ID "CP501_UpgradeWizard_v0202" (or later) or by searching using the following parameters:

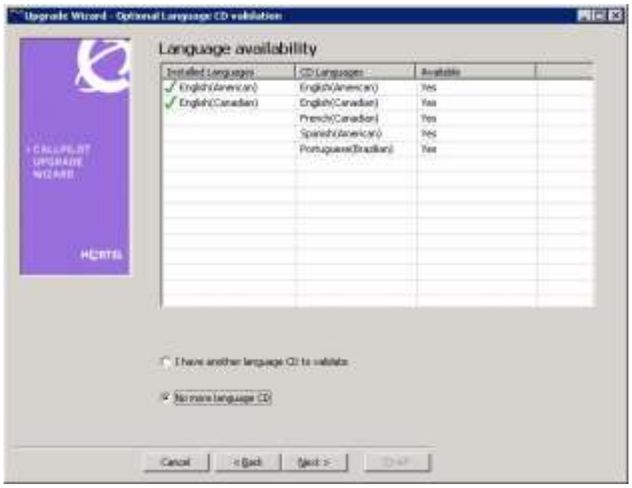
- Product = CallPilot
- Platform = Server
- Release = 5.01.02
- Status = Released

If a previous version of the upgrade wizard has been installed, uninstall it first, then install the latest one.

7.2.1 Language Validation

New functionality was added into the Upgrade Wizard that provides optional validation of the CallPilot 5.0 language CDs plus display currently installed languages. With Upgrade Wizard version 05.01.01.03 and later, if language CD validation is selected, an interactive check of one (1) or more language CDs is possible. Once complete, the list of languages available on all validated CDs is displayed in a table, plus the currently installed languages on the system.

If currently installed languages are missing from the tested language CDs, a Missing Language window is displayed. An example of the currently installed languages being available on the languages CDs being tested is as follows;



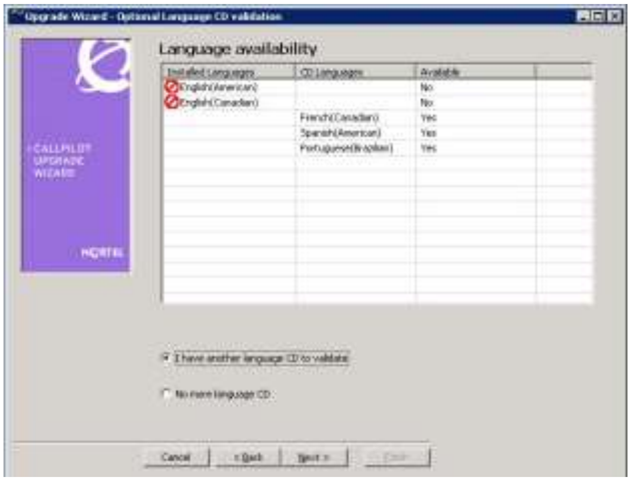
Language availability

Installed Languages	CD Languages	Available
✓ English(American)	English(American)	Yes
✓ English(Canadian)	English(Canadian)	Yes
	French(Canadian)	Yes
	Spanish(American)	Yes
	Portuguese(Brazilian)	Yes

○ I have another language CD to validate

● No more language CD

An example of currently installed languages being unavailable on the language CDs being tested is as follows (2 screens);

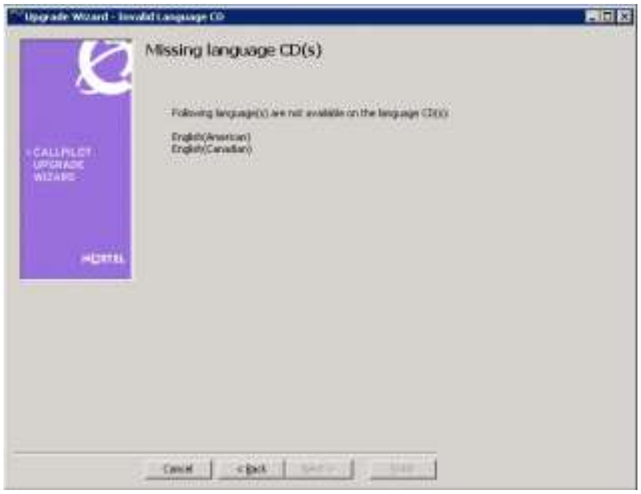


Language availability

Installed Languages	CD Languages	Available
⊘ English(American)		No
⊘ English(Canadian)		No
	French(Canadian)	Yes
	Spanish(American)	Yes
	Portuguese(Brazilian)	Yes

● I have another language CD to validate

○ No more language CD



Missing language CD(s)

Following language(s) are not available on the language CD(s):

English(American)
English(Canadian)

7.3 Setup Wizard and Config Wizard

The Setup Wizard will walk you through the setup of your system. It runs automatically when you reboot your system the first time (and until you have completed it). It will launch Config Wizard at the end. *Do not try to run Config Wizard until the Setup Wizard has been run.*

The first time that you run Internet Explorer (IE) to access CallPilot Manager and the Config Wizard, it will access the Windows Update page.

7.4 Subscriber Manager and CallPilot inter-opt for pass-thru provisioning

7.4.1 Adding a CallPilot Messaging element in UCM

The following steps outline adding an external CallPilot Messaging Element in UCM (only supported when Subscriber Manager is deployed).

1. Log on to UCM as an administrator.
2. In the navigation tree, click Network, Elements. The Elements Web page appears.
3. Click Add. The Add New Element page appears.
4. In the Name field, type the element name. The name must be between 1 to 256 characters in length.
5. In the optional Description field, type a description.
6. Select CallPilot Messaging in the Type list.
7. Click Next. The Add New Element Web page appears for the element.
8. Configure the following CallPilot element types:
    a. CallPilot Manager address: The address for the CallPilot Manager. This field must be a valid IP address or FQDN.
    b. CallPilot server address: The address of the CallPilot Server. This field must be a valid IP address or FQDN.
    c. Administrator mailbox number: The Mailbox number to use when communicating with the CallPilot. CallPilot requires the mailbox number to be from 3- to 18 digits in length; however, the element definition does not enforce this restriction.
    d. Administrator password: The password to use when communicating with the CallPilot. Although CallPilot requires the password to be 4- to 16-digits, the element definition does not enforce this restriction.
9. Click Save. The Elements Web page appears and the new element appears in the list.

7.4.2 Adding a CallPilot certificate to UCM

The Web browser cannot prompt a user to accept a certificate when communicating internally between UCM and CallPilot because CallPilot is not integrated in the UCM security framework.

Use the following procedure to manually add the CallPilot certificate.

1. In the Internet Explorer Web browser, type https://<CallPilot IP>/cpmgr. Where <CallPilot IP> is the IP or FQDN of the CallPilot Manager requiring the certificate.
2. Click View Certificate when prompted with the Security Alert dialog box. The Certificate properties window appears.
3. Select the Details tab and click Copy to File. The Certificate export Wizard window appears
4. Select the Base-64 encoded X.509 (.CER) option and click Next. Type a directory and file name for the certificate and click Next.
5. Click Finish to exit the Certificate Export Wizard.
6. In the navigation tree, click Security, Certificates. The Certificate Management Web page appears.
7. Click the option next to the endpoint for which you want to view the details. In this case, the UCM server.
8. In the Certificate Authorities section, click Add.
9. Open the .CER file from Step 5 in a text editor and copy the contents into the Add a CA to the Service dialog box and click Submit.
10. The CallPilot certificate is displayed in the Certificate Authorities table and all communication to the CallPilot is secured over SSL.

7.5 High Availability

Note: Avaya highly recommends updating all High Availability systems to EMC AutoStart version 5.3 / Service Pack 3 using PEP ID "EMC5.3.3"

7.5.1 Definition File Import Procedure

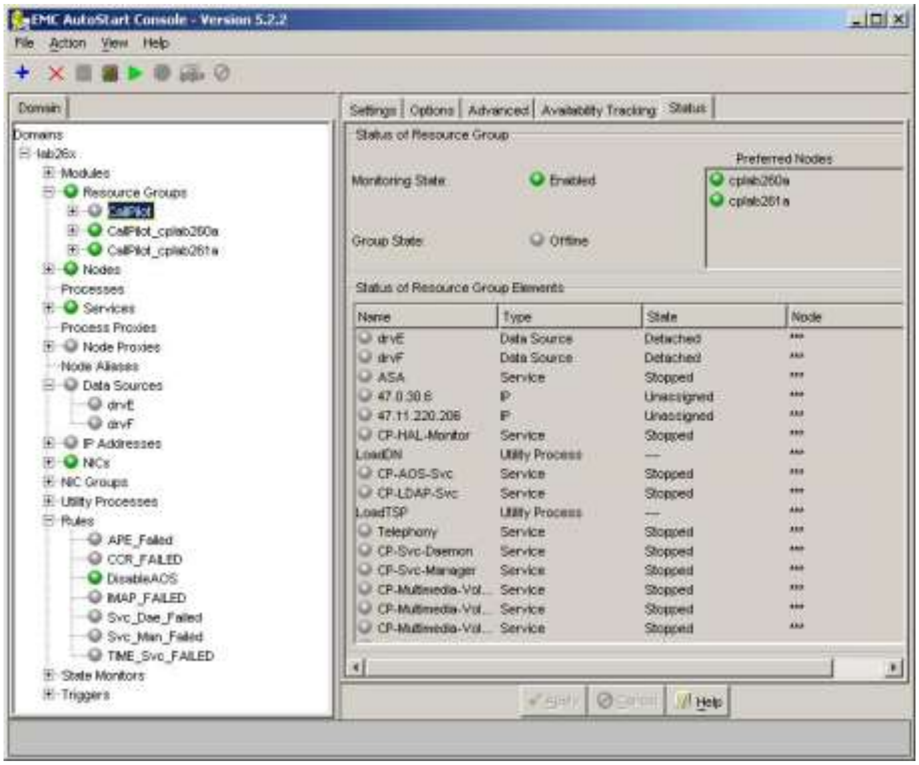
Note: This procedure is only required if the customer High Availability system is currently configured before installing the PEP. This should be in very few cases.

This procedure is to run the PEP, re-create the AutoStart Definition file by running the HA wizard: (HighAvailabilityConfigurationWizard.exe under D:\Nortel\HA) and then re-import the new definition file (*.def under D:\Nortel\HA\ToolkitInstaller2.0) into the AutoStart console.

Once the PEP installations have taken place, this procedure must take place on the same CallPilot server which was used to run the HA wizard the first time as the other files created by the HA wizard. The PEP replaces the Definition Template file with the new parameters. If the wrong system is used, some of the original configuration will be lost.

Process

1. Apply the PEP to the HA servers according to the PEP installation procedure described in the CallPilot 5.0 High Availability NTP NN44200-311.
2. Open the AutoStart Console on the HA server which has the original definition file imported into AutoStart and take the resource group ***CallPilot*** offline if it is online.



Status of Resource Group

Monitoring State: Enabled

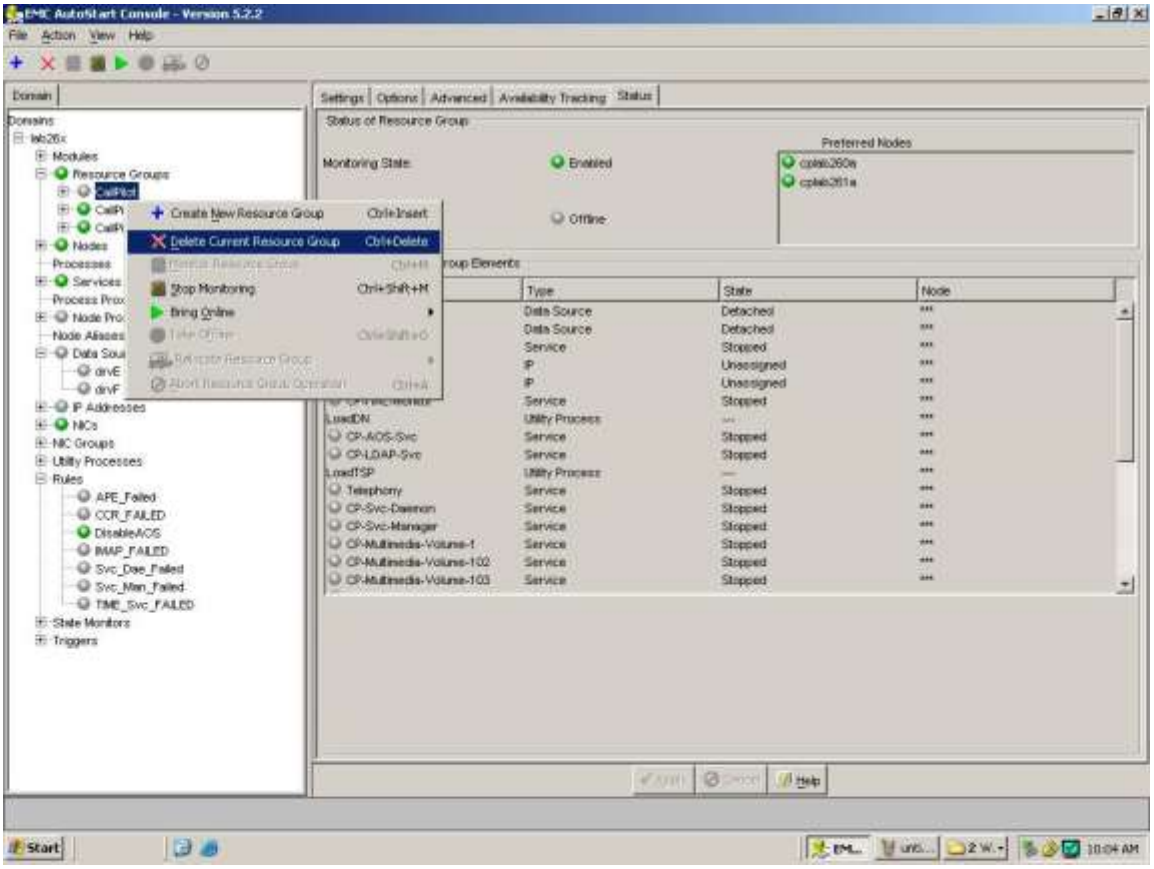
Group State: Offline

Preferred Nodes:
cplab260a
cplab261a

Status of Resource Group Elements

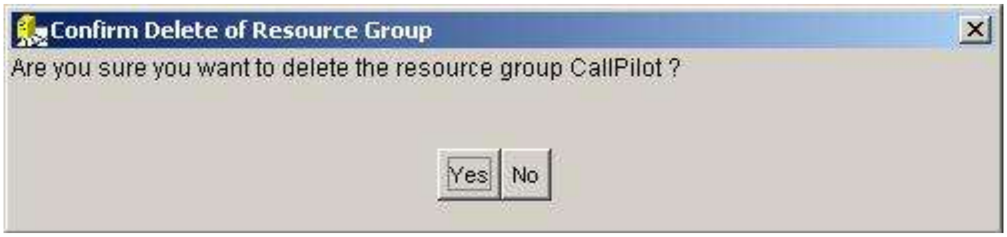
Name	Type	State	Node
drvE	Data Source	Detached	***
drvF	Data Source	Detached	***
ASA	Service	Stopped	***
47.0.30.6	IP	Unassigned	***
47.11.220.206	IP	Unassigned	***
CP-HAL-Monitor	Service	Stopped	***
LoadDN	Utility Process	—	***
CP-AOS-Svc	Service	Stopped	***
CP-LDAP-Svc	Service	Stopped	***
LoadTSP	Utility Process	—	***
Telephony	Service	Stopped	***
CP-Svc-Daemon	Service	Stopped	***
CP-Svc-Manager	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***

3. Expand ***Resource Groups*** on the left panel of the AutoStart Console, and right click the resource group ***CallPilot*** and then click ***Delete Current Resource Group***.



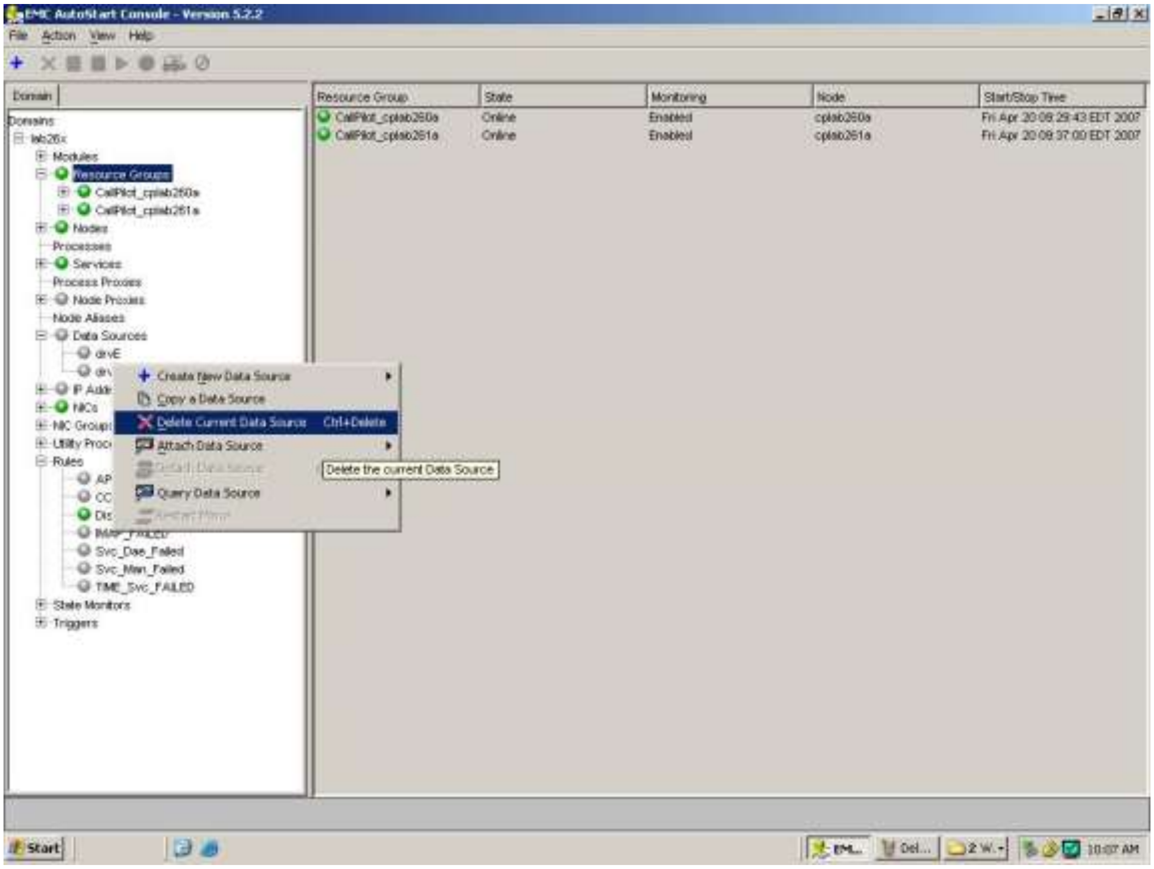
	Type	State	Node
	Data Source	Detached	***
	Data Source	Detached	***
	Service	Stopped	***
	IP	Unassigned	***
	IP	Unassigned	***
	Service	Stopped	***
LoadDN	Utility Process	---	***
CP-AOS-Svc	Service	Stopped	***
CP-LDAP-Svc	Service	Stopped	***
LoadTSP	Utility Process	---	***
Telephony	Service	Stopped	***
CP-Svc-Daemon	Service	Stopped	***
CP-Svc-Manager	Service	Stopped	***
CP-Multimedia-Volume-1	Service	Stopped	***
CP-Multimedia-Volume-102	Service	Stopped	***
CP-Multimedia-Volume-103	Service	Stopped	***

4. Click the **Yes** button on the ***Confirm Delete of Resource Group*** window.



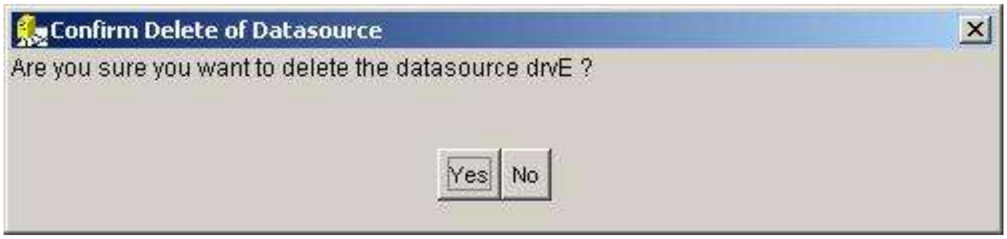
Are you sure you want to delete the resource group CallPilot ?

5. Expand ***Data Sources*** on the left panel of the AutoStart Console, right click on **drvE** and then click ***Delete Current Data Source***.



Resource Group	State	Monitoring	Node	Start/Stop Time
CallPilot_cplab260a	Online	Enabled	cplab260a	Fri Apr 20 08:29:43 EDT 2007
CallPilot_cplab261a	Online	Enabled	cplab261a	Fri Apr 20 08:37:00 EDT 2007

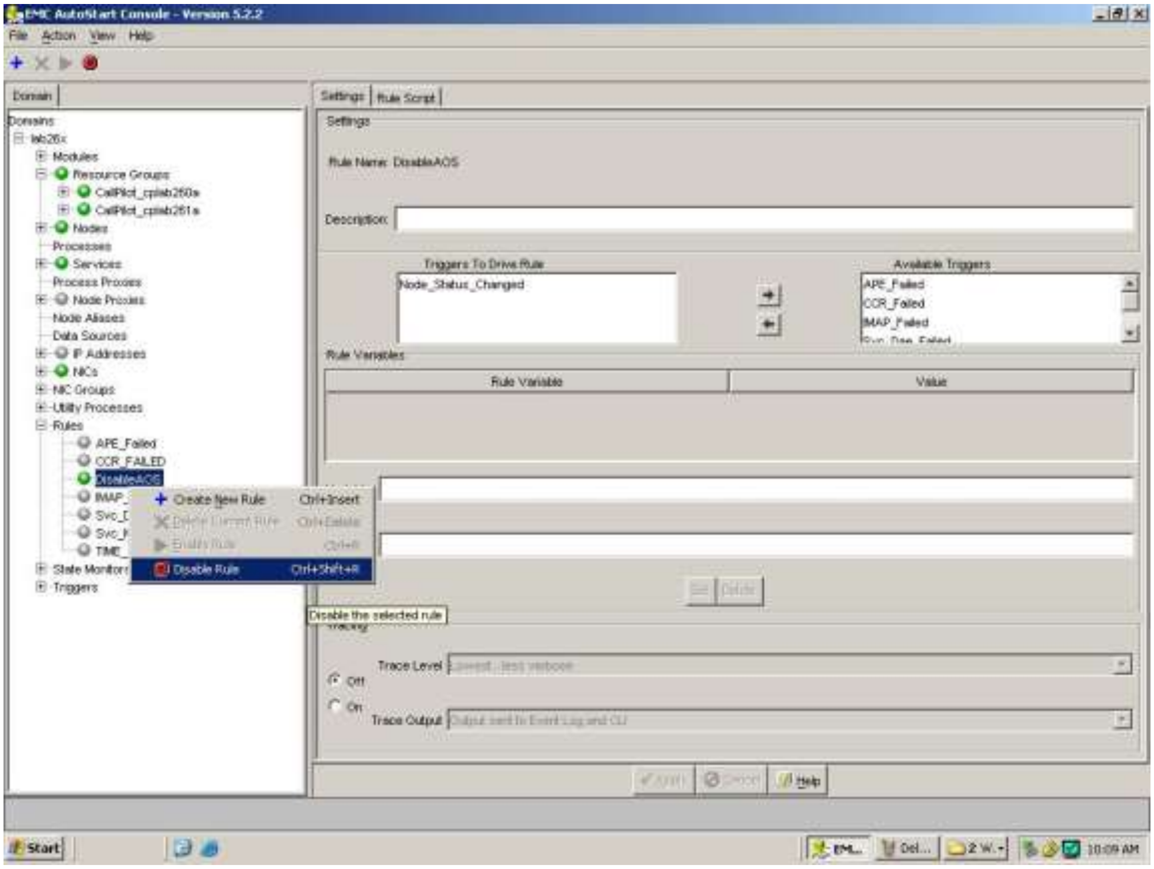
6. Click the Yes button on the ***Confirm Delete of Datasource*** window.



Are you sure you want to delete the datasource drvE ?

7. Repeat the step 4 and 5 on the data source **drvF** to delete drvF as well.

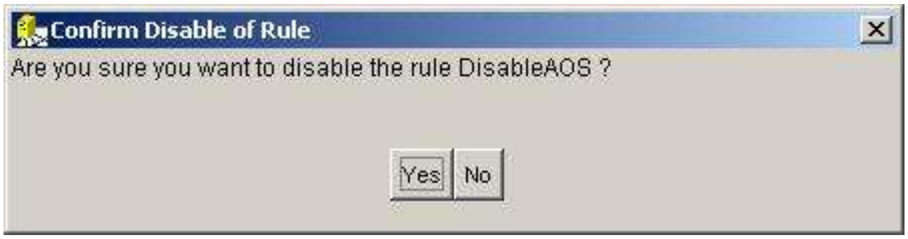
8. Expand ***Rules*** on the left panel of the AutoStart Console, right click ***DisableAOS*** and then click ***Disable Rule*** if the rule ***Disable Rule*** is enabled (in green).



Rule Name: DisableAOS

Triggers To Drive Rule: Node_Status_Changed

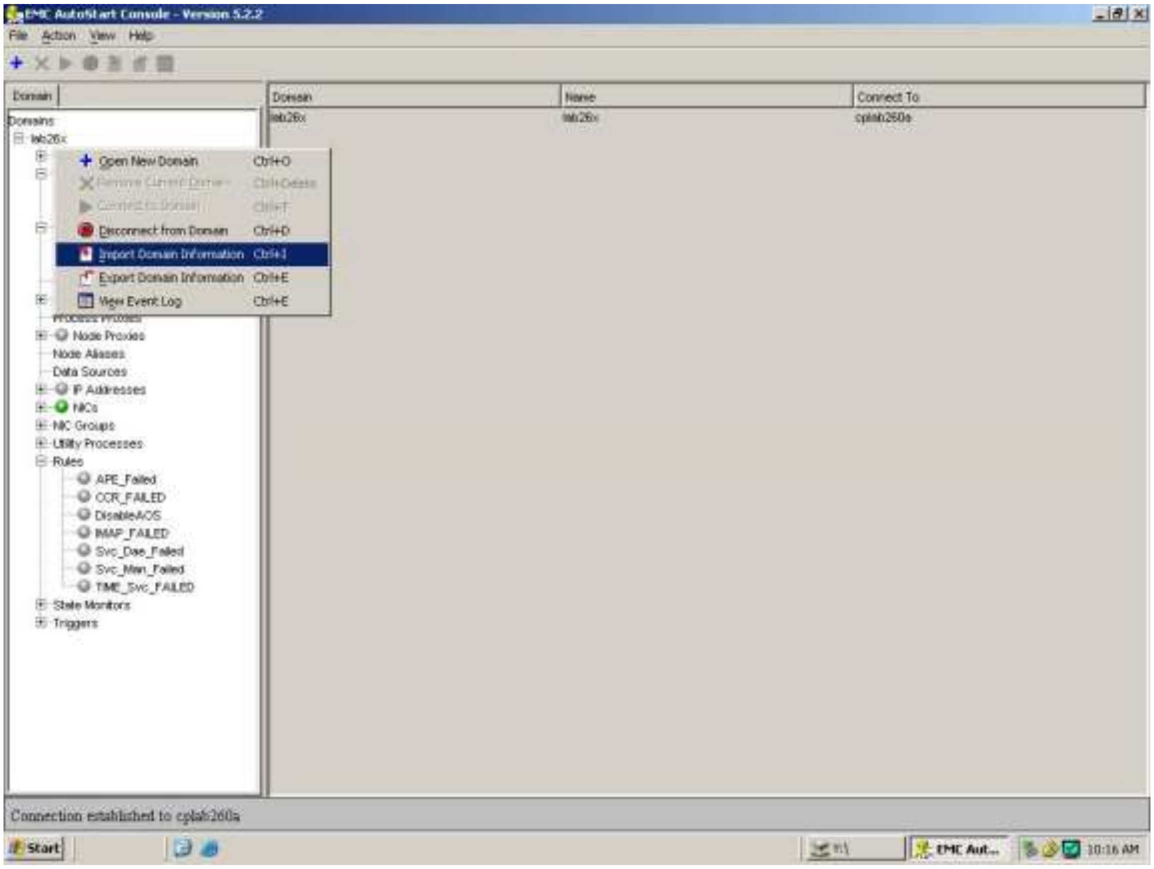
9. Click the **Yes** button on the ***Confirm Disable of Rule*** window.



Are you sure you want to disable the rule DisableAOS ?

10. Launch HighavailabilityConfigurationWizard.exe under D:\Nortel\HA.
11. Click the **Reset** button on the GUI of the High Availability Configuration Wizard. **Note**: Don't close the GUI of the High Availability Configuration Wizard after this step. If you do close the wizard application, you will have to enter the data requested by the High Availability Configuration Wizard again.
12. Click the **Step 1: Get Node Information** button.
13. Click the **Step 2: Validate Node Information** button. The **Stage 1 Complete** window will show up if there is no error.
14. Click the **Ok** button on the **Stage 1 Complete** window.
15. Click the **Exit** button on the GUI of the High Availability Configuration Wizard.

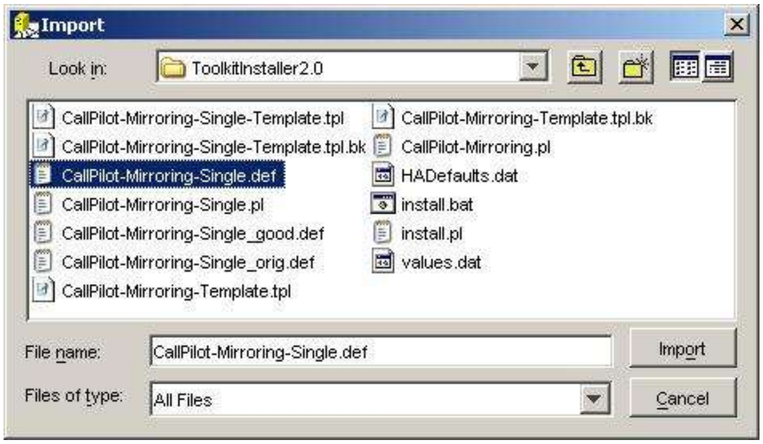
16. Click the **Yes** button on the **Confirm Exit Request** window.
17. Re-launch HighavailabilityConfigurationWizard.exe under D:\Nortel\HA.
18. Click the **Step 3: Generate Definition File** button.
19. Click the **Ok** button of the **Phase 2 Complete** window which will show you the definition file has been successfully generated.
20. Click the **Exit** button, and then click **Ok** button on the **Confirm Exit Request** window to exit the High Availability Configuration Wizard.
21. Open the AutoStart Console if it is open.
22. Right click the AutoStart Domain name (For example, lab26x on the screenshot below) on the top of the left panel of the AutoStart Console, and then click ***Import Domain Information***.



Domain	Name	Connect To
lab26x	lab26x	cplab260a

Connection established to cplab260a

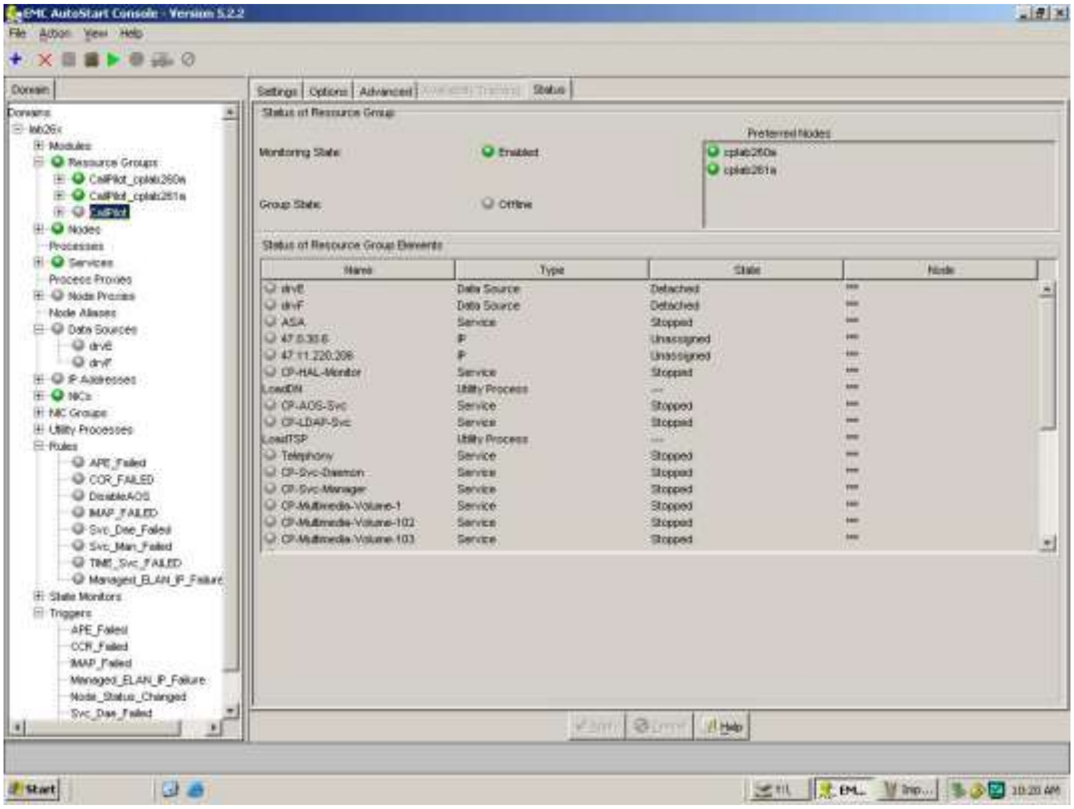
23. Click the new definition file under D:\Nortel\HA\ToolkitInstaller2.0, and then click the **Import** button.


Import
Look in:
ToolkitInstaller2.0
CallPilot-Mirroring-Single-Template.tpl
CallPilot-Mirroring-Single-Template.tpl.bk
CallPilot-Mirroring-Single.def
CallPilot-Mirroring-Single.pl
CallPilot-Mirroring-Single_good.def
CallPilot-Mirroring-Single_orig.def
CallPilot-Mirroring-Template.tpl
CallPilot-Mirroring-Template.tpl.bk
CallPilot-Mirroring.pl
HADefaults.dat
install.bat
install.pl
values.dat
Import
Cancel

File name: CallPilot-Mirroring-Single.def

Files of type: All Files

24. After clicking the Import button and waiting for around one minute, the importing will be succeeded if the Data Sources **drvE**/ **drvF** and the resource group **CallPilot** are created, and there is no error or warning message on the information bar at the bottom of the AutoStart Console. You should check the new item(s) or new setting(s) introduced by the new definition file if there is any, for example, the new trigger ***Managed_ELAN_IP_Failure*** and the new rule ***Managed_ELAN_IP_Failure_Notif*** are created.



Status of Resource Group

Monitoring State: Enabled

Group State: Offline

Preferred Nodes: cplab260a, cplab261a

Status of Resource Group Elements

Name	Type	State	Node
drvE	Data Source	Detached	---
drvF	Data Source	Detached	---
ASA	Service	Stopped	---
47.0.30.6	IP	Unassigned	---
47.11.220.206	IP	Unassigned	---
CP-HAL-Monitor	Service	Stopped	---
LoadDN	Utility Process	---	---
CP-AOS-Svc	Service	Stopped	---
CP-LDAP-Svc	Service	Stopped	---
LoadTSP	Utility Process	---	---
Telephony	Service	Stopped	---
CP-Svc-Daemon	Service	Stopped	---
CP-Svc-Manager	Service	Stopped	---
CP-Multimedia-Volume-1	Service	Stopped	---
CP-Multimedia-Volume-102	Service	Stopped	---
CP-Multimedia-Volume-103	Service	Stopped	---

25. Expand ***Utility Processes*** on the left panel of the AutoStart Console, and update the Login Info (Password, Domain name, and User name) on the Settings tab of each utility process under ***Utility Processes*** (**DisableAOS**, **KillServices**, **LoadDN**, **LoadTSP**, **UnloadTSP**, and **UnloadTSPOnSandbyServer**) by following the procedure **Add the Windows administrator password for the AutoStart UtilityProcesses** in Chapter 5 of CallPilot 5.1 High Availability NTP (NN44200-311).
26. Bring the resource group ***CallPilot*** online by following the procedure **Bring the Resource Groups online** in Chapter 5 of CallPilot 5.1 High Availability NTP (NN44200-311).

7.5.2 CallPilot Switch Ping Email Address Configuration

This procedure describes the configuration of one of more email addresses to whom email messages will be sent when a ping test from CallPilot to the switch fails. If no email accounts are manually configured, the trigger will still fire but no messages sent.

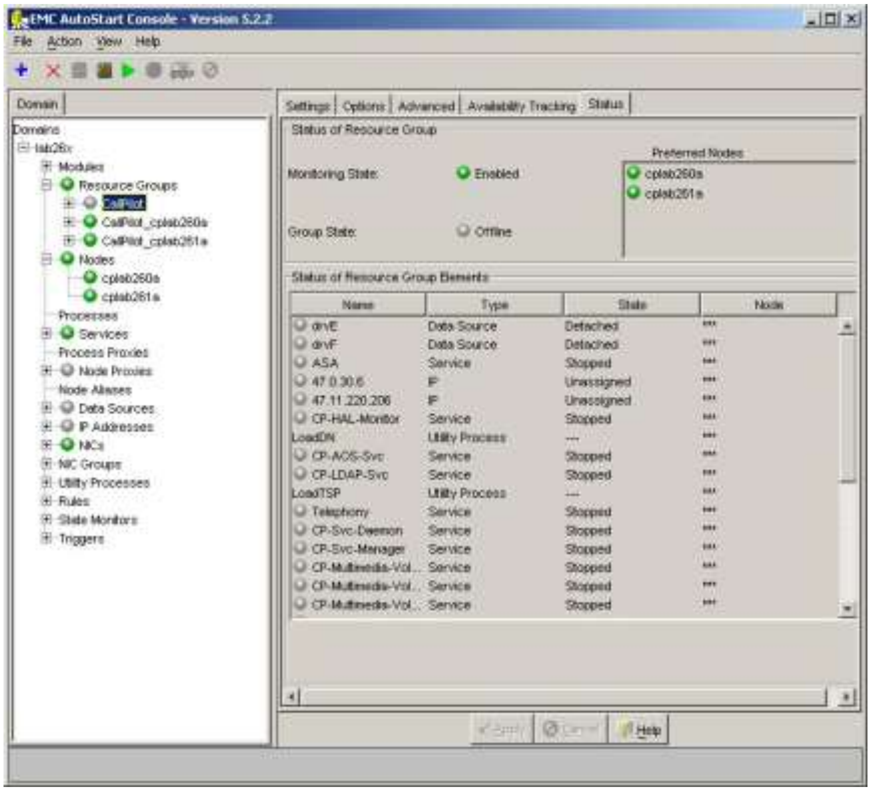
The email addresses are added into a script for the rule Managed_ELAN_IP_Failure_Notif so that AutoStart sends out email notification to administrator(s) when a path test failure occurs for the Managed ELAN IP.

Customers may make this configuration update right after the NTP NN44200-311 procedure ‘Add the Windows administrator password for the AutoStart Utility Processes’ in the section ‘Configure the AutoStart software’ on page 109. This procedure may be executed during a fresh installation after importing the definition file created by the HA wizard, or afterwards on a configured running system.

The email message that will be sent to the email address is; ‘Managed ELAN IP has failed a ping on the HA node CPServerX’ where CPServerX is the active server name of the high availability pair.

1. Make sure that the PEP has been installed on your CallPilot server following the PEP installation procedure described in the CallPilot 5.1 High Availability NTP NN44200-311.

2. Open AutoStart Console, and take the resource group CallPilot offline if it is currently online.



Status of Resource Group

Monitoring State: Enabled

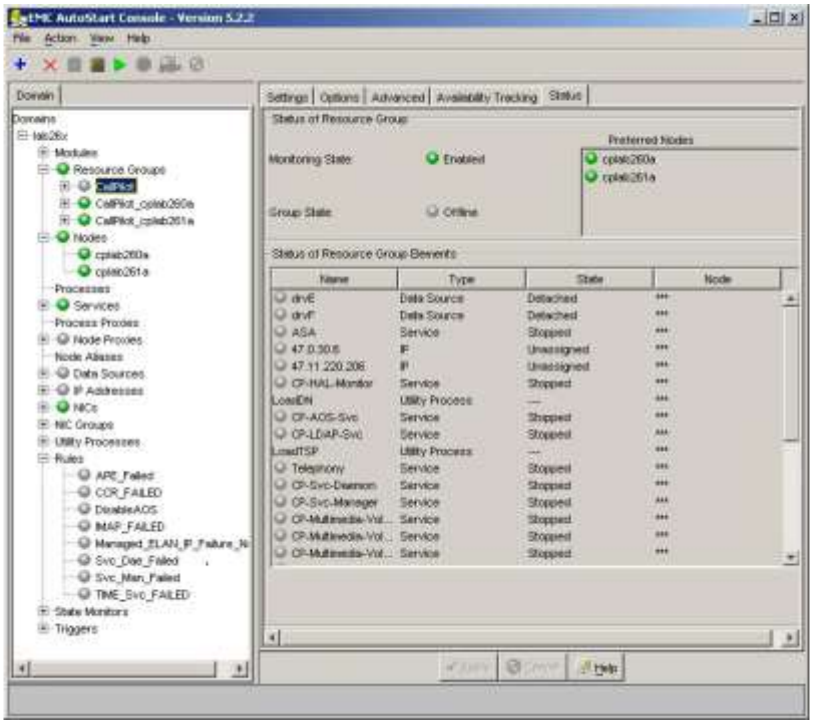
Group State: Offline

Preferred Nodes
cplab260a
cplab261a

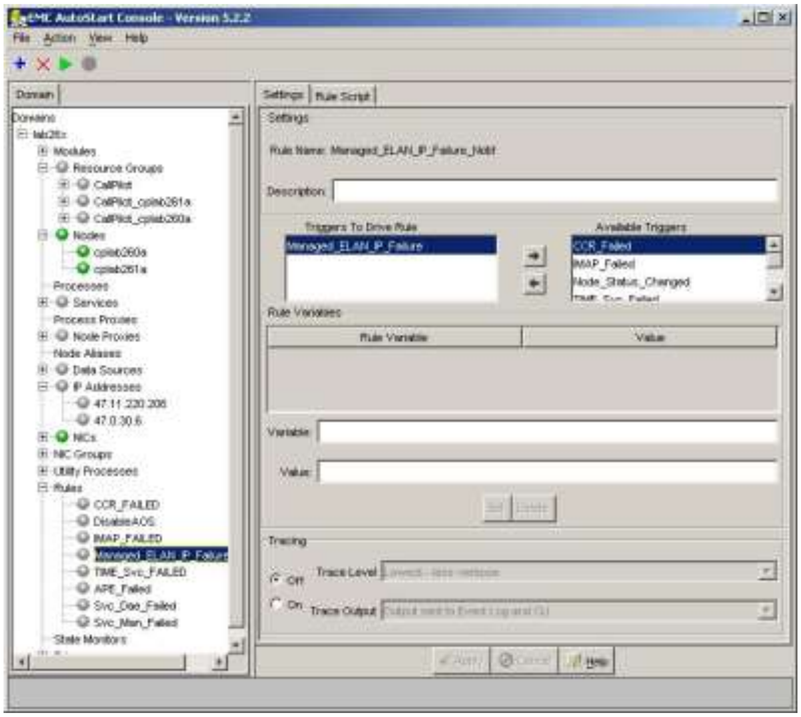
Status of Resource Group Elements

Name	Type	State	Node
drvE	Data Source	Detached	***
drvF	Data Source	Detached	***
ASA	Service	Stopped	***
47.0.30.6	IP	Unassigned	***
47.11.220.206	IP	Unassigned	***
CP-HAL-Monitor	Service	Stopped	***
LoadDN	Utility Process	---	***
CP-AOS-Svc	Service	Stopped	***
CP-LDAP-Svc	Service	Stopped	***
LoadTSP	Utility Process	---	***
Telephony	Service	Stopped	***
CP-Svc-Daemon	Service	Stopped	***
CP-Svc-Manager	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***

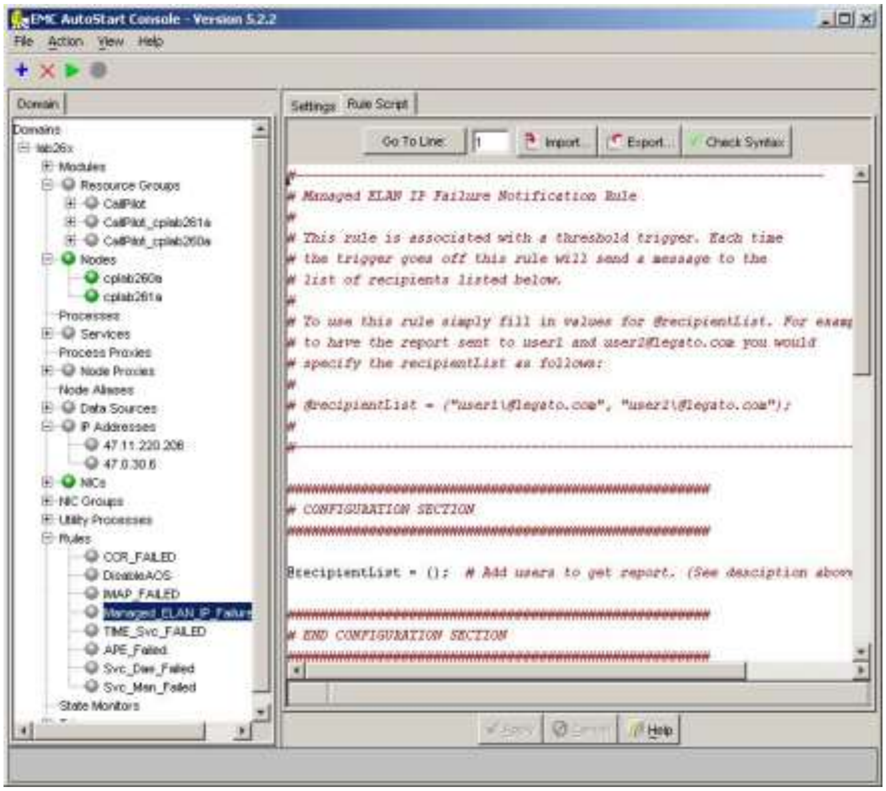
3. Expand *Rules* on the Domain window (The left window of the AutoStart Console).



4. Click the rule Managed_ELAN_IP_Failure_Notif and the window below will appear on the screen.



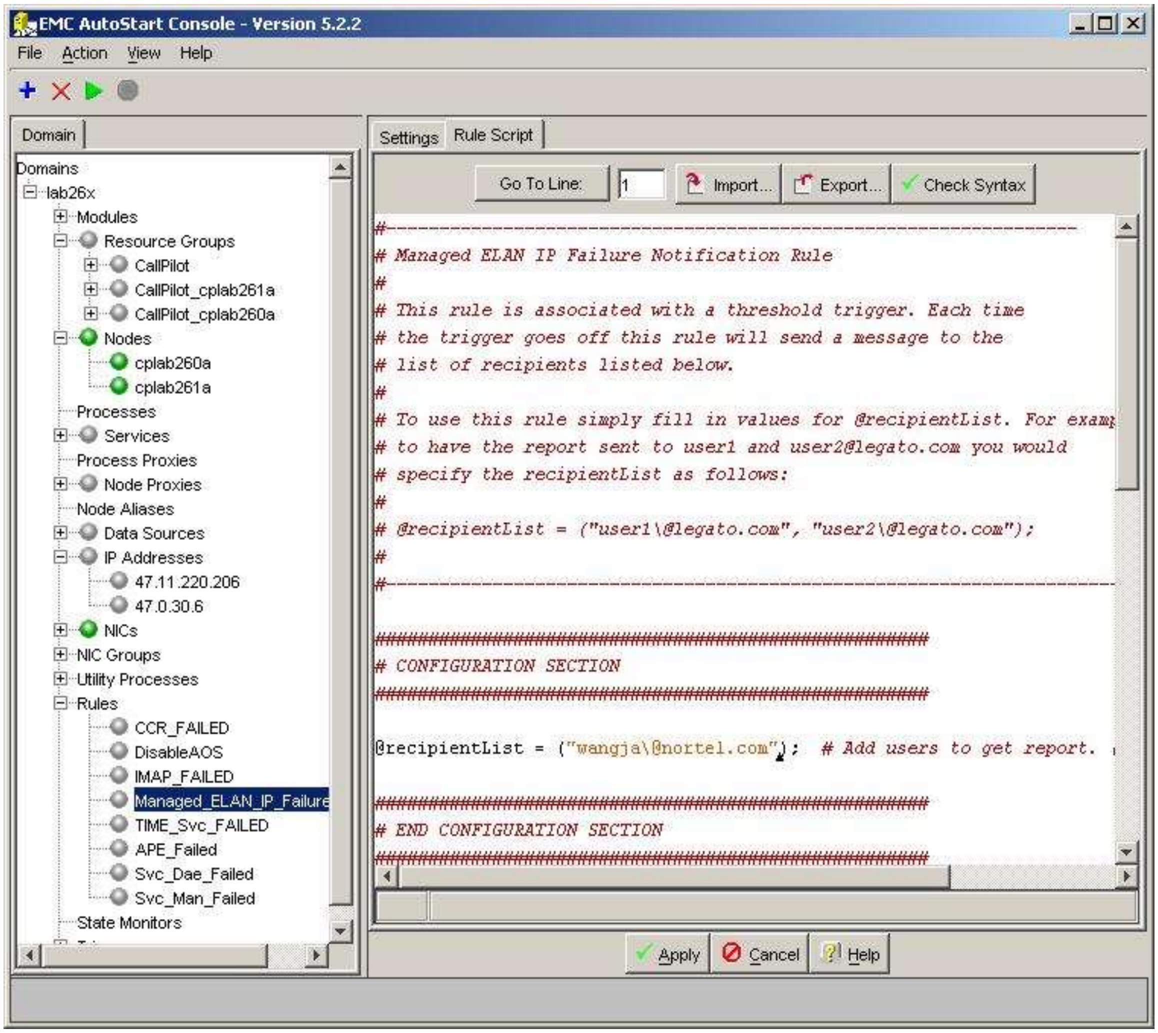
5. Click the *Rule Script* tab, and the rule's script will appear on the right window of the AutoStart Console.



```
#-------------------------------------------------------------------------------
# Managed ELAN IP Failure Notification Rule
#
# This rule is associated with a threshold trigger. Each time
# the trigger goes off this rule will send a message to the
# list of recipients listed below.
#
# To use this rule simply fill in values for @recipientList. For examp
# to have the report sent to user1 and user2@legato.com you would
# specify the recipientList as follows:
#
# @recipientList = ("user1\@legato.com", "user2\@legato.com");
#
#----------------------------------------------------------------------------------


##################################################################
# CONFIGURATION SECTION
##################################################################

@recipientList = ();  # Add users to get report. (See desciption above

##################################################################
# END CONFIGURATION SECTION
##################################################################
```

6. Add the recipient's email address into () of the recipientList in the script by following the required format of email address, and then click the Apply button.

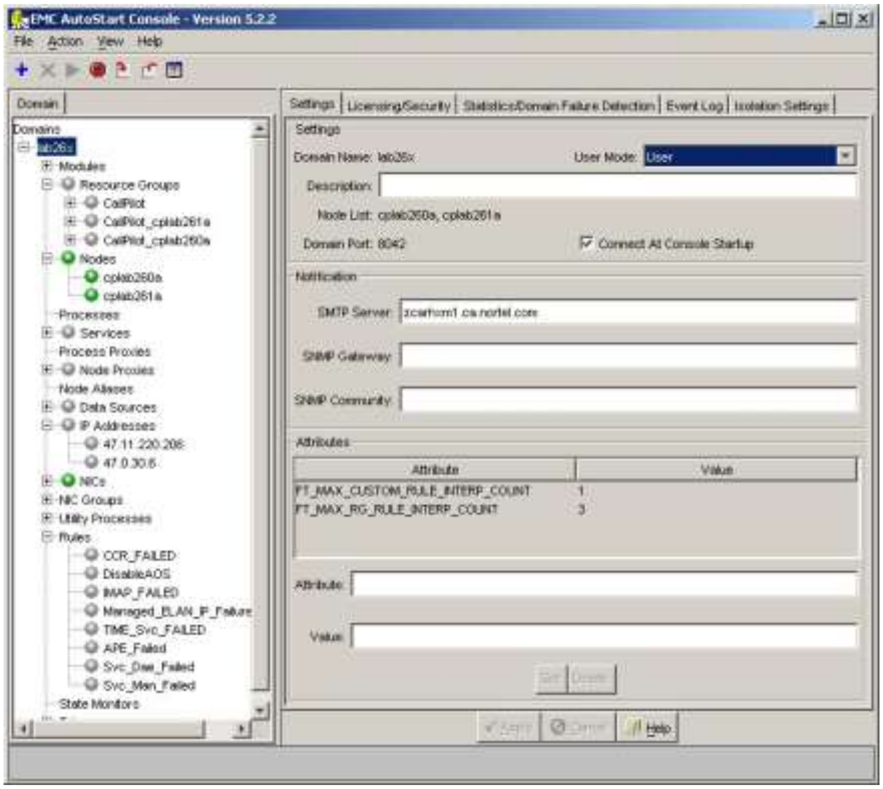
   Note: You have to add "\" before @ inside each email address. Multiple email addresses must be separated by commas.



```
#-----------------------------------------------------------------
# Managed ELAN IP Failure Notification Rule
#
# This rule is associated with a threshold trigger. Each time
# the trigger goes off this rule will send a message to the
# list of recipients listed below.
#
# To use this rule simply fill in values for @recipientList. For exam
# to have the report sent to user1 and user2@legato.com you would
# specify the recipientList as follows:
#
# @recipientList = ("user1\@legato.com", "user2\@legato.com");
#
#--------------------------------------------------------------------


##########################################################
# CONFIGURATION SECTION
##########################################################

@recipientList = ("wangja\@nortel.com");  # Add users to get report.

##########################################################
# END CONFIGURATION SECTION
##########################################################
```

7. Bring the resource group CallPilot online if you took it offline at the beginning of this procedure, or you can continue the installation and configuration procedure in the CallPilot 5.1 High Availability NTP if this is a fresh installation.

8. You also have to configure the SMTP Server of Notification under the Settings tab of the AutoStart Domain on AutoStart Console, as shown in the following screenshot (Click your AutoStart Domain name on the left panel of the AutoStart Console, and then click the Settings tab on the right panel).



Settings

Domain Name: lab26x

User Mode: User

Description:

Node List: cplab260a, cplab261a

Domain Port: 8042

☑ Connect At Console Startup

Notification

SMTP Server: zcarhxm1.ca.nortel.com

SNMP Gateway:

SNMP Community:

Attributes

Attribute	Value
FT_MAX_CUSTOM_RULE_INTERP_COUNT	1
FT_MAX_RG_RULE_INTERP_COUNT	3

Attribute:

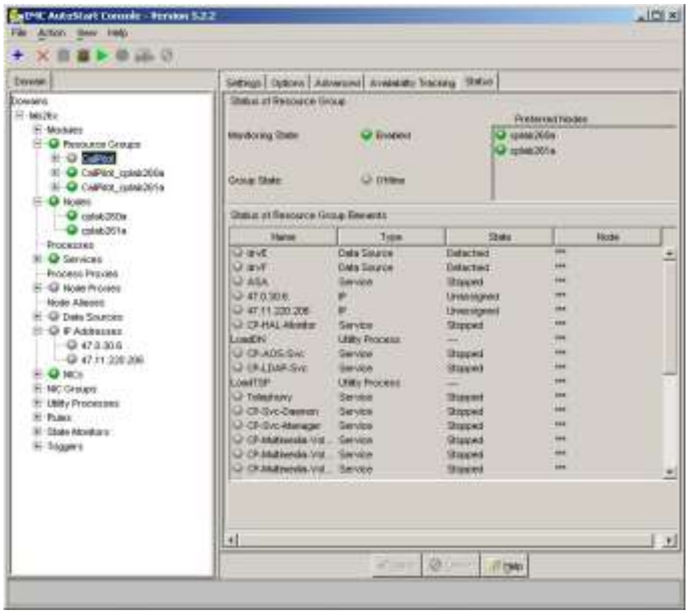
Value:

7.5.3 Enable HA Failover on Switch Ping Failure Procedure

By default the switch ping path test is disabled when the PEP is installed. This procedure describes the enabling of the rule. The process may also be used to disable the rule if enabled.

1. Make sure that the PEP has been installed on your CallPilot server following the PEP installation procedure described in the CallPilot 5.1 High Availability NTP NN44200-311.

2. Open AutoStart Console, expand *Resource Groups* and take resource group CallPilot offline.



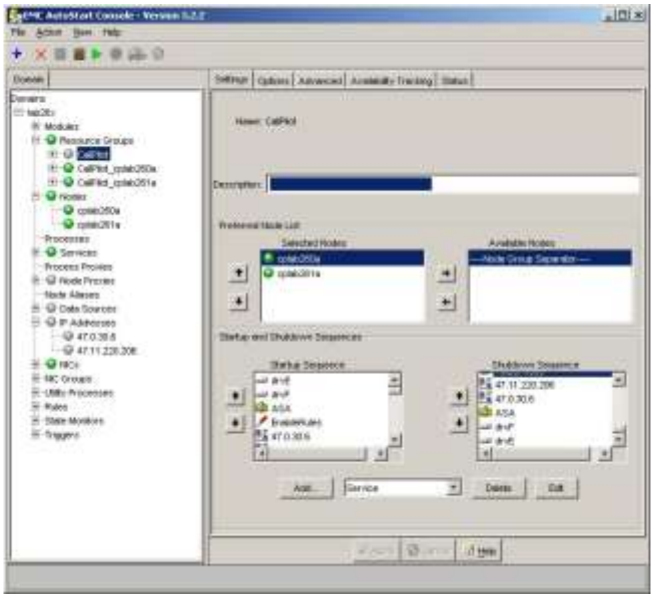
Monitoring State: Enabled

Group State: Offline

Preferred Nodes: cplab260a, cplab261a

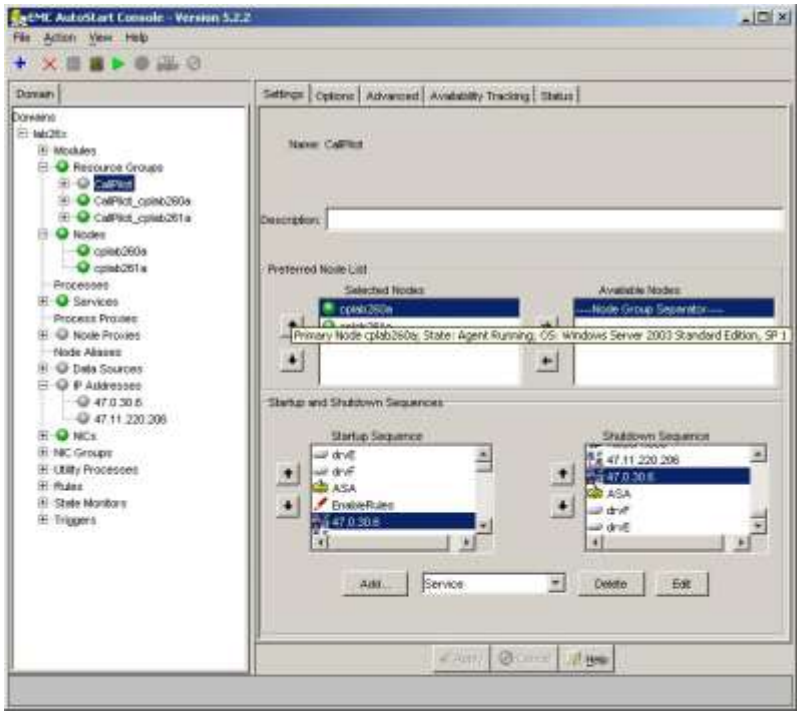
Name	Type	State	Node
drvE	Data Source	Detached	***
drvF	Data Source	Detached	***
ASA	Service	Stopped	***
47.0.30.6	IP	Unassigned	***
47.11.220.206	IP	Unassigned	***
CP-HAL-Monitor	Service	Stopped	***
LoadDN	Utility Process	---	***
CP-ADS-Svc	Service	Stopped	***
CP-LDAP-Svc	Service	Stopped	***
LoadTSP	Utility Process	---	***
Telephony	Service	Stopped	***
CP-Svc-Daemon	Service	Stopped	***
CP-Svc-Manager	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***
CP-Multimedia-Vol...	Service	Stopped	***

3. Click the Settings tab of resource group CallPilot on the right window of AutoStart Console.



Name: CallPilot

4. Highlight the Managed ELAN IP (for example, 47.0.30.6), and click Edit.



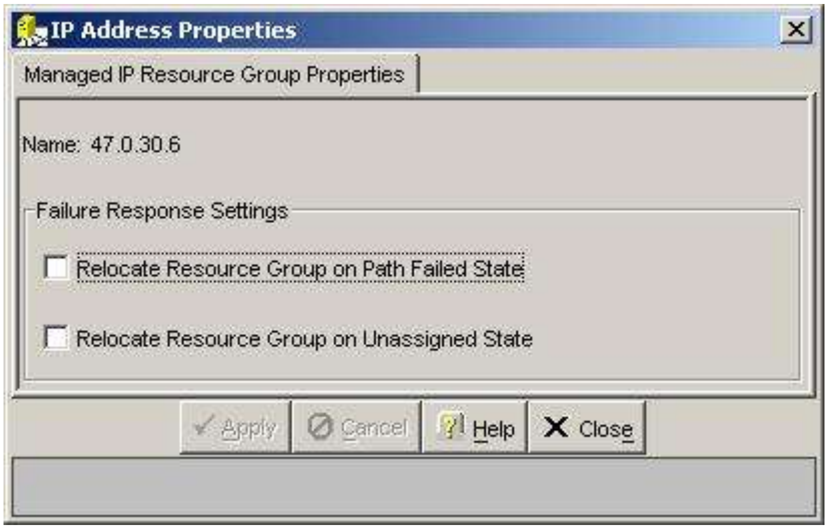
Name: CallPilot

Primary Node cplab260a; State: Agent Running; OS: Windows Server 2003 Standard Edition, SP 1

Startup Sequence: drvE, drvF, ASA, EnableRules, 47.0.30.6

Shutdown Sequence: 47.11.220.206, 47.0.30.6, ASA, drvF, drvE

5. The window below will show up on the screen.

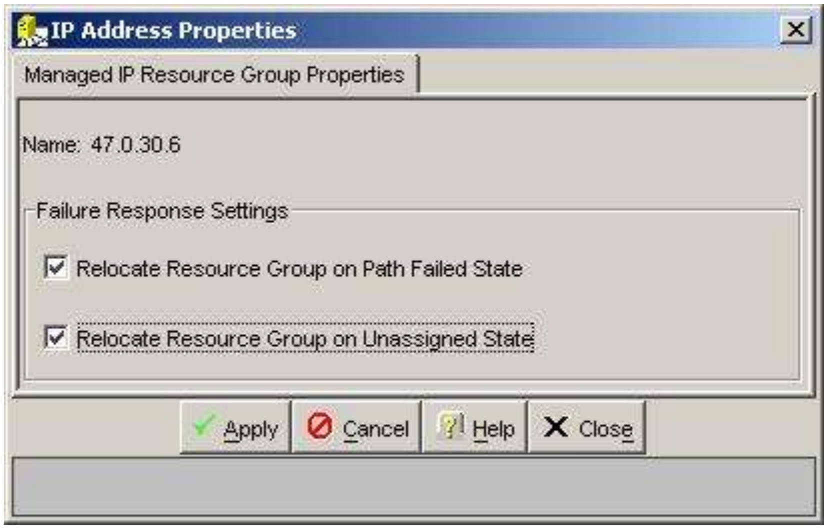

IP Address Properties
Managed IP Resource Group Properties
Failure Response Settings
Apply
Cancel
Help
Close

Name: 47.0.30.6

☐ Relocate Resource Group on Path Failed State

☐ Relocate Resource Group on Unassigned State

6. Check both check boxes on the window and click Apply.



Name: 47.0.30.6

Failure Response Settings

☑ Relocate Resource Group on Path Failed State

☑ Relocate Resource Group on Unassigned State

7. Bring the resource group ***CallPilot*** online by following the procedure **Bring the Resource Groups online** in Chapter 5 of CallPilot 5.1 High Availability NTP (NN44200-311).

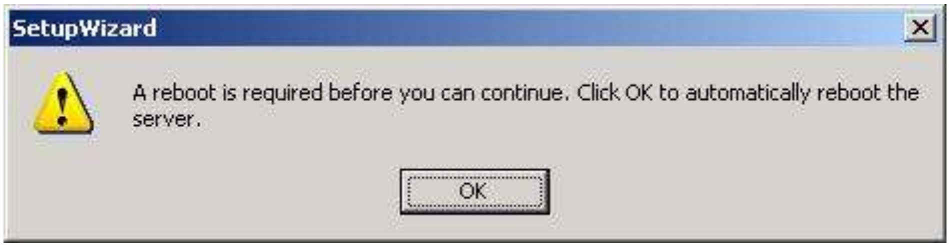
7.6 PEPs

Important: Ensure that you download any PEPs for CallPilot 5.1 (release 05.0.01) and install them when prompted during the Setup Wizard.

> **Note:** After installing 5.1 or booting up a new system for the first time, the Setup Wizard will walk you through setting up you CallPilot. It will prompt you when to install PEPs.
>
> *At this point, the Windows Server 2003 network configuration has not been defined.* If you plan on downloading PEPs from ESPL, either configure your network settings from the control panel, or download the PEPs on another PC that has a network connection and burn them to a CD (recommended).

7.7 Reboot After Setup Wizard

When you have completed the Setup Wizard the system will automatically reboot the server before running the Config Wizard. Prior to the reboot, the following popup will appear. Click OK to reboot the server.



A reboot is required before you can continue. Click OK to automatically reboot the server.

Important: If the server does not start shutting down after a few seconds – a manual reboot may be required.

7.8 Changes in T1/SMDI and CallPilot Server Configuration

Interaction between a CallPilot Server and an SL-100 switch may result in a "glare" condition if the SL-100 places an incoming call to a T1 channel and the CallPilot places an outgoing call to the same T1 channel at the same time. This is akin to two cars traveling in opposite directions, on the same lane of a highway.

This glare is the result of the switch and CallPilot Server, independently of one another, selecting what they see as an idle channel to make a call. When the same channel is selected by both sides simultaneously, a glare condition takes place resulting in a failed call attempt or delayed answering.

To minimize glare conditions, the following configuration guidelines should be adhered to. All T1 channels will be divided into two separate groups to minimize using the same channels for incoming and outgoing traffic. Using different UCD groups on the SL-100 switch for outgoing and incoming calls will eliminate the "glare" condition completely. One of two UCD groups should be used for incoming calls to CallPilot. The second UCD group can be safely used for outbound services.

To split the channels on the CallPilot server side, one additional parameter was added to the T1 channels configuration. That parameter defines the direction of calls that are allowable for the specified group. Channels can be used for incoming calls only, for outgoing calls only or for both types of calls (bidirectional channels).

Bidirectional channels should not be used. The glare condition is only possible if/when there are configured bidirectional channels. Using partitioned incoming and outgoing channels result in decreasing system capacity, and as such, care should be taken when engineering channels that are reserved for inbound and outbound services.

Traffic reports can be used to get statistical information related to number of incoming and outgoing calls. The maximum number of channels that are necessary for incoming and outgoing calls should be defined.

SL-100 Switch Configuration:

Each group of channels on the CallPilot Server has to be associated with a UCD group on the switch. The number of UCD groups has to be the same as the number of groups on CallPilot.

CallPilot Server configuration:

The ability to configure a "Direction" parameter for T1 channels was added into Configuration Wizard starting from CallPilot 5.1.

A drop-down list called "Direction" was added to the SDN Detail Information page in Configuration Wizard. It can have one of three values: "Incoming calls", "Outgoing calls", "Bidirectional". To add a new group, it is necessary to define "Group DN", "Application type" and "Direction" parameters.

7.9 Re-installation of Software

At times you may be required to remove and install or re-install various CallPilot related components. The following is a list of these components. Uninstalling the CallPilot 5.1 server software is supported. Reinstall of the CallPilot 5.1 software is still supported.

7.9.1 CallPilot Manager Install

To install, re-install, or upgrade CallPilot Manager, download the latest version from ESPL.

7.9.2 AppBuilder Install

To install, re-install, or upgrade CallPilot Application Builder, download the latest version from ESPL.

7.9.3 Directory Sync MMC Plug-in

The Directory Sync MMC plug-in install executable (plug-in.exe) can be found in the \DirectorySync folder on the root of the CallPilot Applications CD.

7.9.4 CallPilot Server Reinstall

Re-installing CallPilot server via Application CD is supported. The CallPilot Server reinstall executable (setup.exe) can be found in \CallPilotInstall folder on the root of the CallPilot Application CD.

Note: While Reinstalling the CallPilot software, you may receive a Windows File Protection' error. You should choose the option to continue using the questionable (from Windows point of view) file.

7.9.5 Adobe Reader 7 uninstall / install / reinstall

Found in \AdobeReader7. Run "Change" from the control panel -> Add / Remove programs to repair an existing installation and run "Remove" to uninstall. Run the executable AdbeRdr70_enu_full.exe, and follow the on screen instruction to reinstall. The default installation directory is: C:\Program Files\Adobe\Acrobat 7.0.

IMPORTANT NOTE: For CallPilot 5.1 systems, it is recommended to not install Adobe Reader 7, but rather upgrade to Adobe Reader 9.3. Reference Product Advisory Alert bulletin PAA-2010-0006-Global / CallPilot Security Update – Adobe Reader.

<u>Obtaining Adobe Reader 9.3.</u>
Using a separate client PC, download the "Adobe Reader 9.3 update – Multiple languages" (dated 01/12/2010) from the Adobe website, under "Downloads" and "Adobe Reader for Windows".
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows
(Note: URL is subject to change).

Notes:

- Using a separate PC avoids the need to add Adobe as a trusted website on the CallPilot server.
- When installing Adobe Reader 9.3, the installation may offer the chance to install additional software such as toolbars or other extras. DO NOT INSTALL ANY EXTRAS. Be sure to install only Adobe Reader 9.3.
- Once installed, from the "Edit" menu, select "Preferences", then select "JavaScript" category. Uncheck box "Enable Acrobat JavaScript" (this reduces exposure to future security problems). Click OK and exit out of Adobe Reader.

7.9.6 LSI MegaRaid 1600/320-2 Power Console + (RAID admin software)

This software is only applicable to the 703t and 1002rp platforms.

Found in \RAID\MegaRaidPowerConsole. Run "Change" from the control panel -> Add / Remove programs to repair an existing installation. Run "Remove" to uninstall. Run the executable setup.exe, and follow the on screen instruction to reinstall. The default installation directory is: C:\Program Files\MegaRAID.

7.10 Change in location of various Windows OS-centric utilities

In Windows Server 2003, Microsoft has relocated many OS-centric utilities that may be used for installation, configuration, or maintenance of the CallPilot server. The following highlights those commonly used utilities and how to access then in Windows Server 2003

- **Event Viewer:** Start > Programs > Administrative Tools > Event Viewer
- **Disk Management:** Start > Programs > Administrative Tools > Computer Management
- **Device Manager:** Start > Programs > Administrative Tools > Computer Management
- **Local Users and Groups:** Start > Programs > Administrative Tools > Computer Management
- **Services:** Start > Programs > Administrative Tools > Services
- **Computer Name:** <Use Configuration Wizard>. Do not change the computer name via the Operating System otherwise database inconsistencies may result.

7.11 SSL certificate installation on the CallPilot server

Note: The following information will be included in a future edition of NTP NN44200-601 / Avaya CallPilot Administrator Guide.

Internet Information Server (IIS) on the CallPilot server is preconfigured to use a self-signed "CallPilotWebServiceCert" certificate for Secure Sockets Layer (SSL) connections. This certificate can be replaced with any self-signed and/or purchased SSL certificate on the CallPilot server.

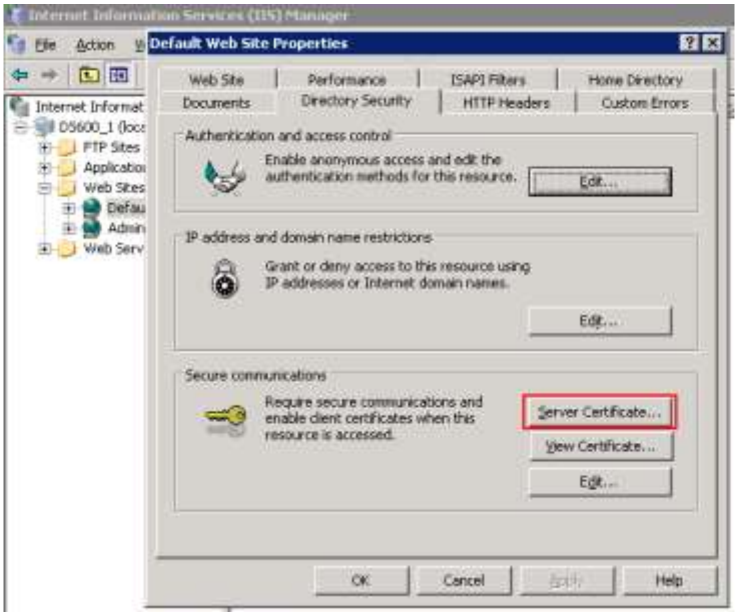
Before administrators can select security options, you need an additional SSL certificate for use with the IIS.

- Entrust (http://www.entrust.net/index.htm)
- Verisign (http://www.verisign.com/)

To install the SSL certificate on the CallPilot server

Note: It is assumed you have a certificate in .pfx format as well as password for it. If you have certificate in any other forms, please contact your certificate provider for instructions about this certificate installation.

1. Open IIS Manager.
2. Select Default Web Site, Properties, Directory Security, Server Certificate.

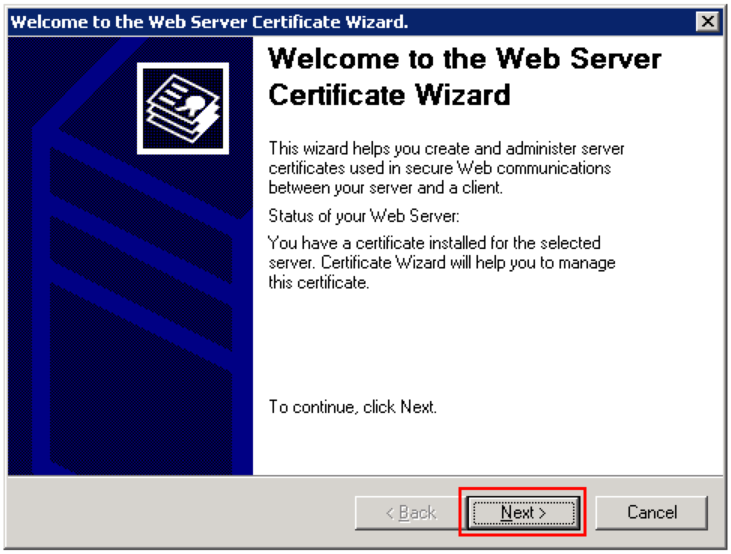


Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or Internet domain names.

Require secure communications and enable client certificates when this resource is accessed.

3. This will start the certificate wizard. Click "Next".


Welcome to the Web Server Certificate Wizard.
Welcome to the Web Server Certificate Wizard
< Back
Next >
Cancel

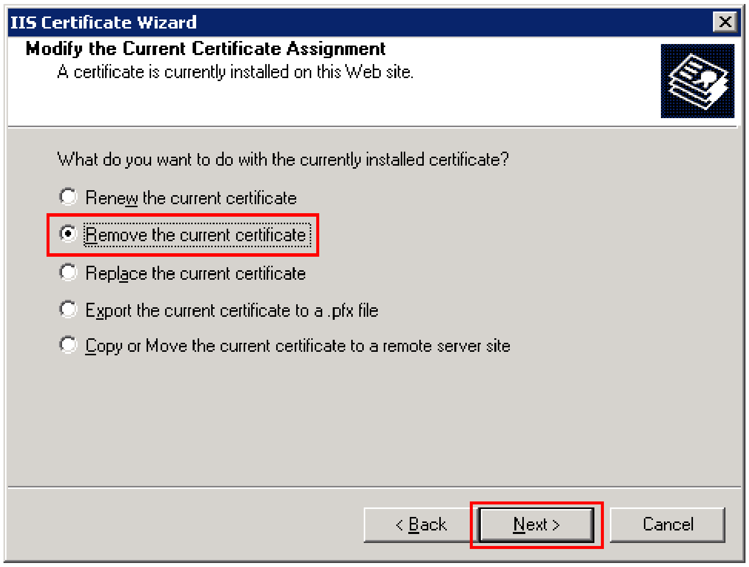
This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

Status of your Web Server:

You have a certificate installed for the selected server. Certificate Wizard will help you to manage this certificate.

To continue, click Next.

4. Select the "Remove the current certificate" option and click "Next".

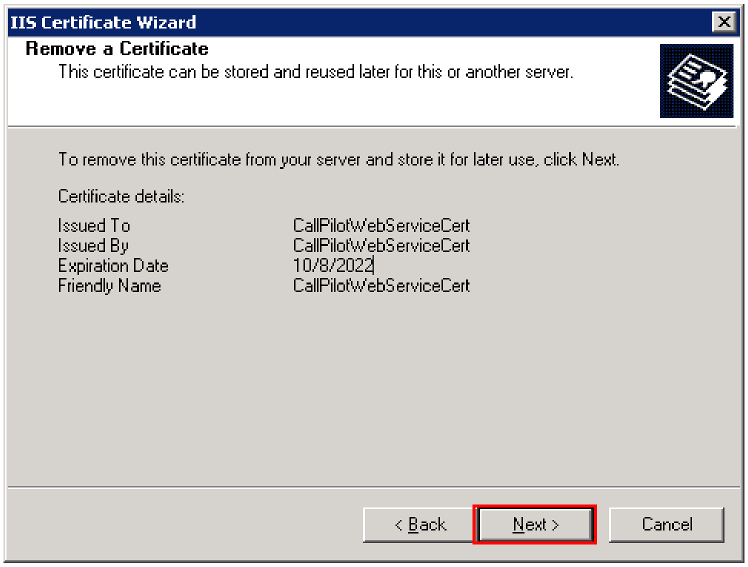


A certificate is currently installed on this Web site.

What do you want to do with the currently installed certificate?

○ Renew the current certificate
● Remove the current certificate
○ Replace the current certificate
○ Export the current certificate to a .pfx file
○ Copy or Move the current certificate to a remote server site

5. Click “Next” again to confirm.



Remove a Certificate

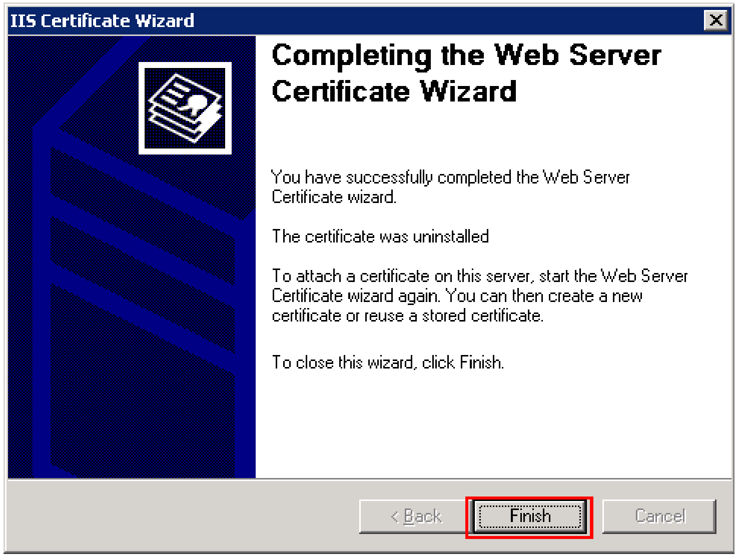
This certificate can be stored and reused later for this or another server.

To remove this certificate from your server and store it for later use, click Next.

Certificate details:

Issued To	CallPilotWebServiceCert
Issued By	CallPilotWebServiceCert
Expiration Date	10/8/2022
Friendly Name	CallPilotWebServiceCert

6. Click “Finish”.



Completing the Web Server Certificate Wizard

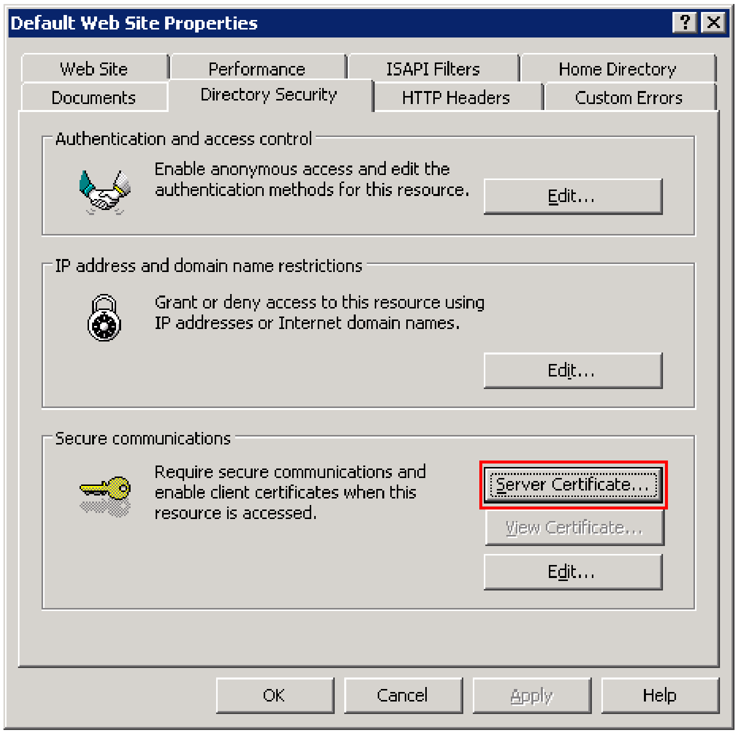
You have successfully completed the Web Server Certificate wizard.

The certificate was uninstalled

To attach a certificate on this server, start the Web Server Certificate wizard again. You can then create a new certificate or reuse a stored certificate.

To close this wizard, click Finish.

7. Click the “Server Certificate” button again.

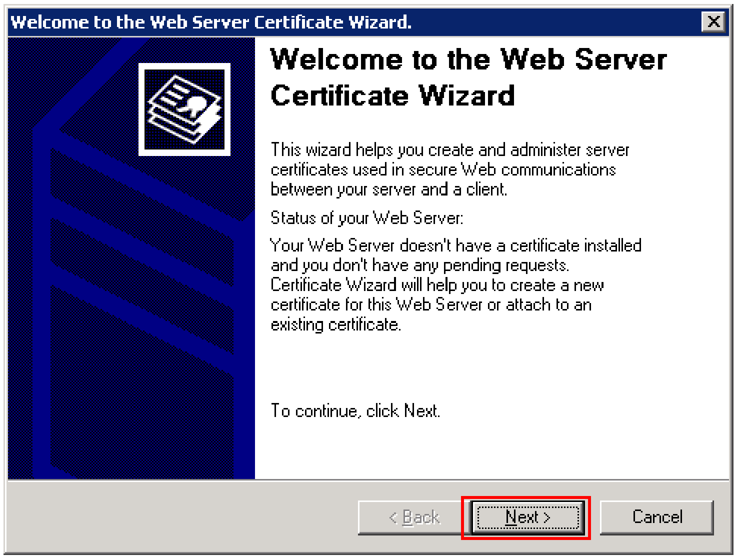


Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or Internet domain names.

Require secure communications and enable client certificates when this resource is accessed.

8. This will start the certificate wizard. Click "Next".



Welcome to the Web Server Certificate Wizard

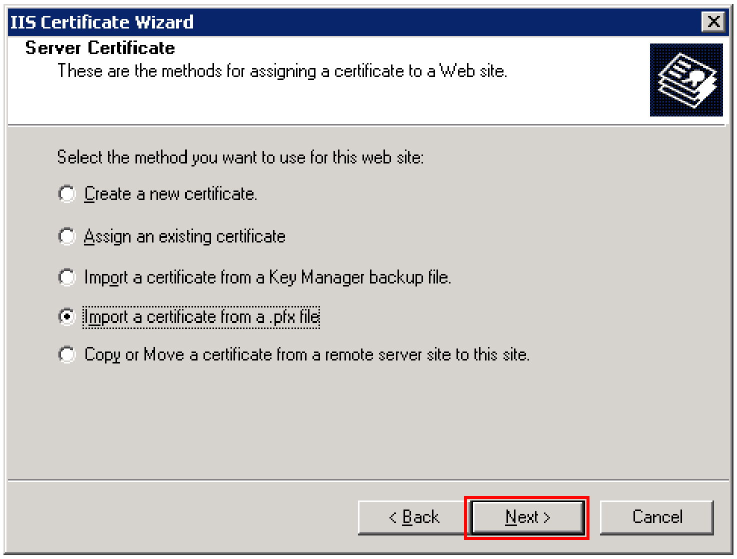
This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

Status of your Web Server:

Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate.

To continue, click Next.

9. Select the “Import certificate from a .pfx file” option and click “Next”.

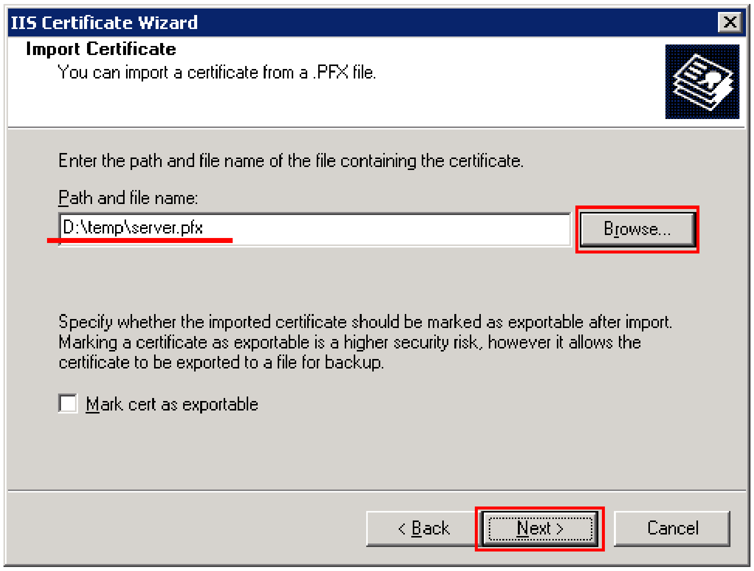


IIS Certificate Wizard
Server Certificate
These are the methods for assigning a certificate to a Web site.
< Back
Next >
Cancel

Select the method you want to use for this web site:

○ Create a new certificate.
○ Assign an existing certificate
○ Import a certificate from a Key Manager backup file.
● Import a certificate from a .pfx file
○ Copy or Move a certificate from a remote server site to this site.

10. Click the “Browse…” button, navigate to your certificate, and click “Next”.



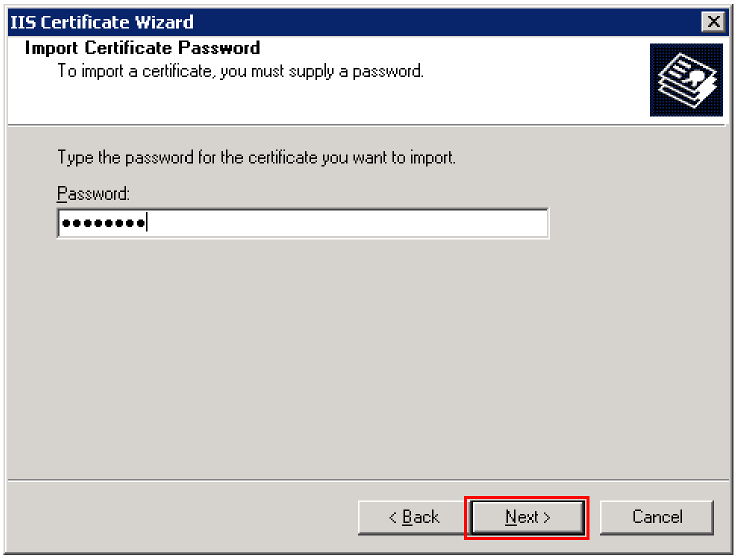
Enter the path and file name of the file containing the certificate.

Path and file name: D:\temp\server.pfx

Specify whether the imported certificate should be marked as exportable after import. Marking a certificate as exportable is a higher security risk, however it allows the certificate to be exported to a file for backup.

☐ Mark cert as exportable

11. Type your password and click “Next”.



IIS Certificate Wizard

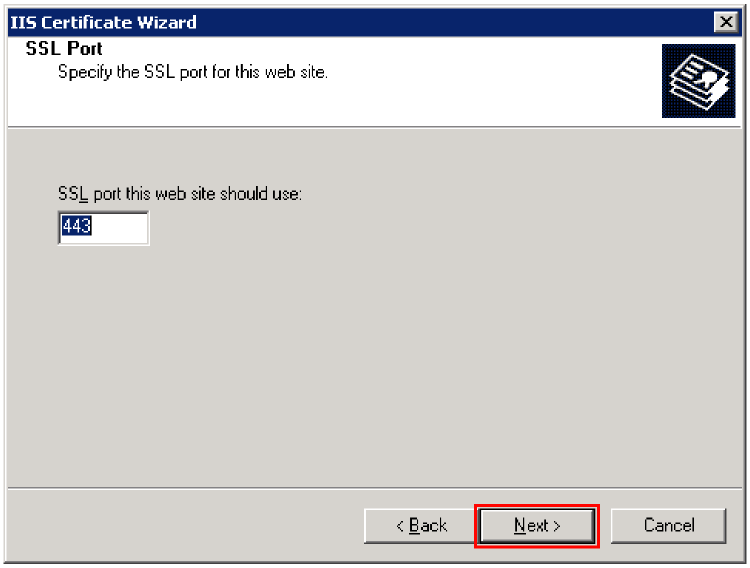
Import Certificate Password

To import a certificate, you must supply a password.

Type the password for the certificate you want to import.

Password: ••••••••••

12. Click “Next”.



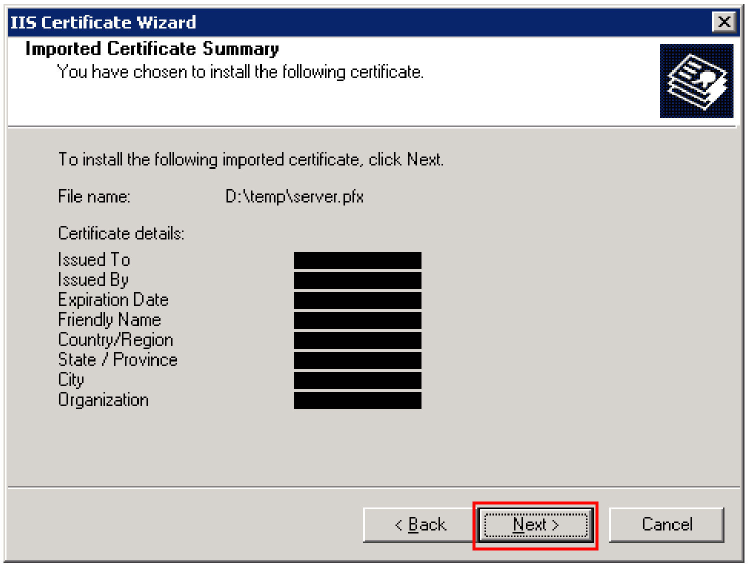
IIS Certificate Wizard

SSL Port

Specify the SSL port for this web site.

SSL port this web site should use: 443

13. Click “Next”.



Imported Certificate Summary

You have chosen to install the following certificate.

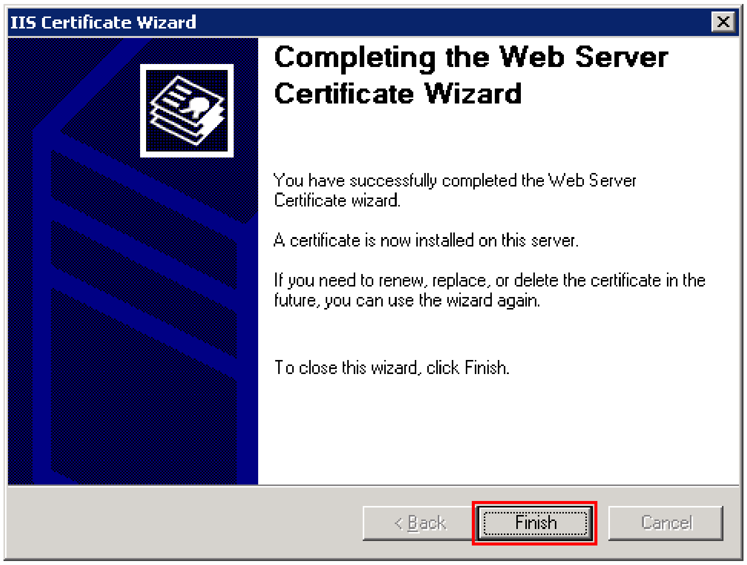
To install the following imported certificate, click Next.

File name: D:\temp\server.pfx

Certificate details:

Issued To	[redacted]
Issued By	[redacted]
Expiration Date	[redacted]
Friendly Name	[redacted]
Country/Region	[redacted]
State / Province	[redacted]
City	[redacted]
Organization	[redacted]

14. Click “Finish”.



Completing the Web Server Certificate Wizard

You have successfully completed the Web Server Certificate wizard.

A certificate is now installed on this server.

If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.

To close this wizard, click Finish.

7.12 SSL certificate removal from the CallPilot server

To remove the SSL certificate from the Windows certificate store

Important: Do not remove certificate you are currently use for SSL connections. Do not remove any unknown certificates. It may cause unpredictable issues.

1. Click on the Start menu and click Run.
2. Type in mmc and click OK.
3. Click on the File menu and click Add/Remove Snap-in...
4. Click on the Add button. Double-click on Certificates.
5. Click on Computer Account and click Next.
6. Leave Local Computer selected and click Finish.
15. Click the Close button. Click OK.
16. Click the plus sign next to Certificates in the left pane.
17. Click the plus sign next to the Personal folder and click on the Certificates folder.
18. Right-click on the certificate you would like to delete and select Delete. Click Yes.

7.13 Avaya Policy on Domain Configuration

Changes to CallPilot Server, including via Group Policy

CallPilot is a turn-key unified messaging server consisting of proprietary software pre-installed on specific proprietary hardware platforms provided by Avaya. Some of the supported hardware platforms were released several years ago with earlier versions of the CallPilot product software and continue to be able to run the latest software releases. These platforms have sufficient hardware resources to support the full CallPilot application capacity but are limited when compared with newer hardware platforms.

The CallPilot product supports a wide range of standard and proprietary interfaces to allow it to communicate with telephone switching equipment, user desktops, other CallPilot systems and other network servers. The rich functionality of a CallPilot server is fully tested and supported by Avaya.

CallPilot currently uses the "Appliance" version of the Microsoft Windows Server 2003 operating system, which comes pre-installed, pre-activated, pre-configured, pre-engineered and pre-hardened on the CallPilot hardware. Customers purchasing the CallPilot product are not required to have expertise in engineering, configuring and hardening servers. Avaya documentation describes how to perform needed system administration and maintenance operations but does not provide the internal implementation details that would be required if customers were to be able to re-engineer or re-configure their CallPilot servers.

In order to ensure the reliable operation of a CallPilot system, and to ensure that trained support personnel can quickly resolve any problems, Avaya has long had the policy that it cannot support CallPilot systems that have had unauthorized configuration changes made by customers. The supported configuration is the one that has been verified by Avaya testing and is the one which Avaya ensures can be properly updated, upgraded, feature-expanded and remotely supported. Windows has a large number of configuration settings. Avaya has found that customer changes to these settings, although they may be well-meaning attempts to improve system security or performance, often result in unexpected downtime or system degradation when applied to a CallPilot server.

By default, CallPilot servers do not participate in a domain. In response to customer requests, Avaya now allows customers to join their CallPilot servers as members into their Windows Domain. Unfortunately, some customers have misunderstood this as allowing system reconfiguration to be carried out by applying domain group policies to the CallPilot server.

Group Policy is a convenient way for network administrators to manage large numbers of Windows desktops. It can also be used to manage various classes of servers within the domain. Different specific configurations can be defined using Microsoft's Group Policy tools, for example to cover desktops and different types of servers (e.g. web servers, domain controllers, database servers, file servers). Of course, it is good policy to fully test group policies before applying them to production servers and to conform with vendor guidelines for those servers where applicable.

On a CallPilot server, only a very limited set of parameters are authorized for a customer to change, and therefore only a very limited set of parameters are appropriate for inclusion in a group policy for application on a CallPilot server. Since login passwords are under customer control, password policies for login accounts (i.e. Administrator) can be changed by the customer. Domain user-ids can be added to a CallPilot server. Note that CallPilot has several built-in application user-ids whose passwords must not be changed. (These user-ids have restricted privileges and cannot be used for local login.)

CallPilot servers are remotely supportable using remote control over dial-up or VPN connections. This remote support capability allows rapid resolution of many types of system problems without requiring an on-site visit. Remote access to a customer's system is under the control of the customer. The customer controls the passwords to the user-ids used by support personnel. The customer can choose to unplug the dial-up line from the remote support modem for greater security when there is no need for remote support. When remote support is required, however, the support personnel do require full administrative access rights to the CallPilot server, including the ability to reboot the system, install device drivers and perform any other needed operation on the server.

As network security has become more and more important, many organizations have developed security hardening rules for the systems on their networks. These rules may have evolved over a number of years and may address security issues in a range of Microsoft OS products, probably making use of recommendations from Microsoft and other 3rd party security consultants and scanning tools for how to securely configure various common types of Windows-based systems. The hardening rules usually specify which OS services should run, what file system permissions should be set, logging and audit policies, web server settings, user rights and many other security-related settings. However, the rules were never developed with consideration for the specific operational requirements of a CallPilot server. CallPilot servers require particular services to run and require other configuration settings that differ from other types of common servers.

Avaya fully recognizes the importance of network security. CallPilot servers are extensively hardened in their default configuration and customers should not attempt to further harden them by applying customer-specific hardening rules. Changing security settings can break CallPilot features, sometimes in unexpected ways. If an actual security vulnerability is suspected in a CallPilot server, Avaya will investigate and address it with a high priority. If a customer has suggestions for improving the security of a CallPilot server, for example by further hardening it, Avaya welcomes such suggestions and, if considered technically feasible, will incorporate suggested improvements in forthcoming CallPilot security PEPs. This process allows the changes to be fully tested and also allows the improvements to be made available to the entire CallPilot customer base.

Please refer to the following NTPs for further details on domain configuration:

- NN44200-302 *Meridian 1 and CallPilot Server Configuration*
- NN44200-303 *Communication Server 1000 and CallPilot Server Configuration*
- NN44200-303 *T1/SMDI and CallPilot Server Configuration*

No customer configuration changes should be necessary on a CallPilot server. Avaya does not recommend any configuration changes. However, the following is a list of minor configuration changes that are authorized for a customer to make. These changes can be made either locally or via Group Policy. If a change is not listed below, it is not authorized and should not be made.

Administrator user-id password may be changed.

Password policies

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements
- Store passwords using reversible encryption (recommended setting is Disabled)

Account Lockout Policy

- Account lockout duration
- Account lockout threshold
- Reset account lockout counter after

Desktop settings. For example:

- Desktop background and appearance
- Screen saver (but do not use a 3D animated screen saver that might consume excessive CPU)
- Folder views
- Creating a shortcut to a program on the desktop or in the start menu

Userids including Domain userids can be added. Customer is responsible for managing these securely. Such userids may later also be deleted.

Temporary files and folders can be removed from under folders D:\TEMP, C:\WINDOWS\TEMP and per User temp folders under Documents and Settings. (NOTE: do not remove the TEMP folders themselves). Temporary Internet files may also be removed.

Certificates may be installed in the IIS web server. IIS settings relating to the use of certificates may be changed to conform to customer PKI requirements.

Windows Update may be used to install authorized hotfixes only. See the bulletin CallPilot Server Security Update.

Adobe Reader may be updated according to the CallPilot bulletin on Adobe Reader updating.

Avaya-released updates to the CallPilot software (e.g. PEPs and SU's) may be installed. Follow instructions in the included readme files.

Just to reiterate, any other configuration changes, whether carried out locally on a CP server or via Group Policy are not authorized. Such changes may impact CallPilot functionality or operation in unexpected ways. Avaya cannot support a CallPilot server on which unauthorized changes have been made. Full system reinstall may be required to resolve any problems that might result.

Here are some examples of configuration changes that must **NOT** be made (This list is not exhaustive – if a change is not explicitly mentioned above, then it is not authorized)

- User Rights must not be changed on any predefined userid or for any user group that contains a predefined userid
- File system permissions must not be changed
- Registry key permissions must not be changed
- Service startup parameters must not be changed
- Unauthorized software must not be installed
- Auditing of file system or registry changes must not be changed
- Installation of unauthorized Anti-Virus software is not allowed. AV software configuration must follow Avaya guidelines for CallPilot.
- Arbitrary registry values must not be changed
- IIS web server settings must not be changed except as detailed above.

7.14 Avaya Policy on network security scans against CallPilot servers

Organizations have an understandable requirement to ensure their networks are as secure as possible against threats. One way to do this is to periodically scan their network hosts using one of a variety of available network security scanners. These scanners do not require any software to be installed on the target hosts and the scanner is not configured with any host-specific passwords. They simulate various types of network attacks that an attacker could make, then typically generate a report detailing any security weaknesses they find. In some cases, organizations are required by law to perform security scanning to check the security of their network.

There are many different security scanners. The exact scan performed by a given security scanner may vary according to the scan parameters that are configured or also, on a day to day basis, according to an ever changing set of vulnerabilities that the scanner is checking for. Therefore, although Avaya does do some internal security vulnerability scanning of CallPilot, it is possible that a customer-initiated scan may impact CallPilot servers in a way that Avaya has not previously encountered.

Network security scanners from reputable vendors are designed to be run in production environments with minimal performance impact on the target hosts. Usually their network traffic load is small, although this can usually be configured to some extent.

Network security scanners should not be confused with software security vulnerability tools that are executed on the target system by a logged on user. Security tools must never be run on production CallPilot servers. Network scanners operate by sending network packets to the target system. They attempt to simulate the kind of malicious attacks that could be made over the network.

CallPilot servers are expected to be able to withstand typical network security scans without service impact. There may, however, be event logs and alarms raised on a CallPilot server indicating protocol errors, invalid login attempts or other minor problems. This is expected and is not a problem. Memory usage, CPU and disk traffic may also spike up during the security scan but should return to normal once the scan is complete. Temporary “low virtual memory” conditions may be observed.

Occasionally, a particular scan might uncover a problem with CallPilot. The scan may impact CallPilot service in an unacceptable way, or the scan might report serious security vulnerability in the CallPilot software. Avaya recommends that CallPilot servers be kept up to date with the latest CallPilot PEPs, (particularly security PEPs), properly configured anti-virus software (see bulletin CallPilot Support for Anti-Virus Applications) and the most recent Microsoft hotfixes (see bulletin CallPilot Server Security Update-<year>, revised periodically, typically monthly). These measures will reduce the chances of a problem resulting from a security scan, as well as, of course, reducing the chances of a real attack being successful.

Since there is some risk of impacting CallPilot service during a scan, Avaya recommends that network security scans should be carried out only during off-peak hours. If a customer does experience a problem with their CallPilot server that seems to be related to the security scan, the customer should check that their scan has been configured in a reasonable way and that their CallPilot server has been properly updated. If the problem persists, the customer can contact support. The support organization should work with the customer to understand the issue and determine whether it is a real product problem. If there is a serious impact to CallPilot operation, it may be necessary to temporarily suspend or modify the scanning of the CallPilot server until a solution can be deployed.

The reports generated by a security scan will usually mention at least some low severity security problems on CallPilot. For example, the reports will often indicate that a web server, FTP server, TAPI, SMTP and DCOM are running. These are normal for a CallPilot server since these services are required to support certain CallPilot features. While it is considered good practice to not run these services if not needed, they do not represent a security problem so long as all applicable patches have been applied. If serious security vulnerability is reported, the customer can contact support to inform Avaya of the problem. Avaya will investigate the reported vulnerability and, if appropriate, will develop a product fix. This process will take some time since full testing will be needed. Customers should not attempt to close a reported vulnerability by making an unauthorized configuration change to their CallPilot server – such changes cannot be supported since they may have undesired, unexpected impact to CallPilot feature operation.

8 Known Problems / Issues

8.1 Server

8.1.1 Server OS Activation

If the server does not have or detect the correct release of the BIOS/firmware, the O/S requires activation after the image is installed. If the system is not activated within 30 days it will be blocked from logging into the Windows Server 2003 system if logged out. Options at that point are:
(1) Activate your system using the COA via the internet or phone, or
(2) Re-image your system for another 30 day trial period.

If after installing an image you adjust the date past the 30 day activation period the system will lock and you will have to activate it or install it from an image again.

Upgraded 703t Tower systems require product activation as part of the upgrade process. All platforms supporting upgrade to CallPilot 5.0 (except the 703t) have the latest BIOS on their respective image media that eliminates the need to activate Windows. The 703t image CD does not have an updated BIOS; therefore Windows Server 2003 activation is required.

Workaround: Ensure the system has the appropriate BIOS/Firmware versions or activate using the supplied COA.

8.1.2 Incorrect Settings in ELAN DNS and WNS

The CallPilot 5.0 image for the 1002rp has incorrect ELAN configuration. The ELAN has IP address settings for the DNS and WNS**.** This may generate unnecessary traffic on the customer's network. Refer to wi00675199.

Workaround: Remove the unwanted values from the ELAN DNS and WINS. From the Control Panel, select Network Settings. Right click on the ELAN connection, and select 'properties'. Select 'TCP/IP' and click on 'properties'. Go to 'Advanced' and select the DNS tab. Remove the values for 'DNS server addresses'. Remove the values for 'DNS suffixes'. Select the 'WINS' tab. Remove the values for 'WINS addresses'

8.1.3 Using Wrong Image CD

Using the wrong image CD/DVD on a server (i.e. 201i on a 1002rp) will cause unpredictable results i.e. the image will install but the system may not work correctly.

Workaround: Only use CallPilot Image CDs that correspond to the matching platform type. Running the Upgrade Wizard will prevent this problem since it will ensure you have correct CD.

8.1.4 Unable to change password via Configuration Wizard

When the "Finish" button is clicked, at the last page in Configuration Wizard dialog, the server is updated with all new information provided by user. During this phase, the Configuration Wizard will try to update the password, but could fail, due to the Windows Server 2003 security policy ("Minimum Password Age") if the policy value is set to a value greater than zero (0).

Workaround: Adjust the Windows Server 2003 security policy for Minimum Password Age to zero (0). This will alter the security policy for this server, so recommend coordinating with the system administrator first.

8.1.5 "No Dongle Found" error after installation

Very intermittently, you may receive a "No Dongle Found" error after installing a 201i server.

Workaround: Reboot the server.

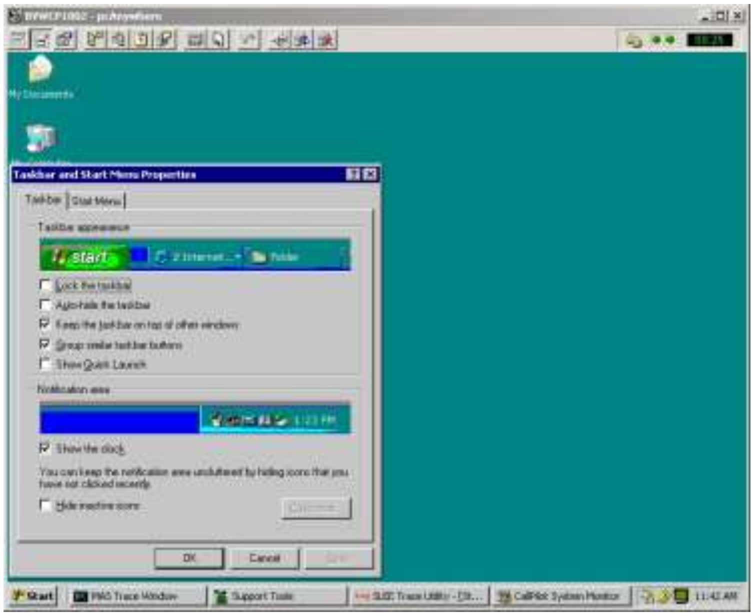
8.1.6 "RDP Protocol Component – Data Encryption" error

When trying to connect to a 201i from a desktop using Microsoft Remote Desktop, the following error "The RDP Protocol component "DATA ENCRYPTION" detected an error in the protocol stream and has disconnected the client." May occur which may block connecting to the server.

Workaround: Refer to Microsoft Knowledge Base article KB323497 at the following URL http://www.support.microsoft.com/?kbid=323497

8.1.7 Taskbar Menu pops up or MAS window appears in center of screen pcAnywhere issue

Whenever the MAS window is minimized, the Taskbar Menu pops up as indicated (see below). Additionally, sometimes closing the Taskbar Menu results in the MAS window appearing in the center of the screen again. This behavior is primarily observed when using pcAnywhere. Refer to CR # Q00947757.



☐ Lock the taskbar
☐ Auto-hide the taskbar
☑ Keep the taskbar on top of other windows
☑ Group similar taskbar buttons
☐ Show Quick Launch
☑ Show the clock

You can keep the notification area uncluttered by hiding icons that you have not clicked recently.

☐ Hide inactive icons

8.1.8 Windows Task Bar appears to be missing

When the system is first powered up following a new install, the mini-setup will run for a period of time and then reboot. Once the system reboot has completed, you will be able to log into the system using one of the CallPilot Windows usernames. Once logged in, the Windows taskbar may appear to be missing but is only hidden at the bottom of the console window. Refer to wi00683107. No fix planned from Microsoft.

Workaround: To make the taskbar visible, use your mouse pointer and left mouse button to grab the task bar and pull it up to the desired height.

8.1.9 Remote Disk backup to network share takes excessively long time

When performing remote disk backups to a network share, if the LAN configuration is invalid, the backup may still complete successfully, but may take a longer period of time.

Workaround: To ensure the NIC is configured appropriately, use the following steps:

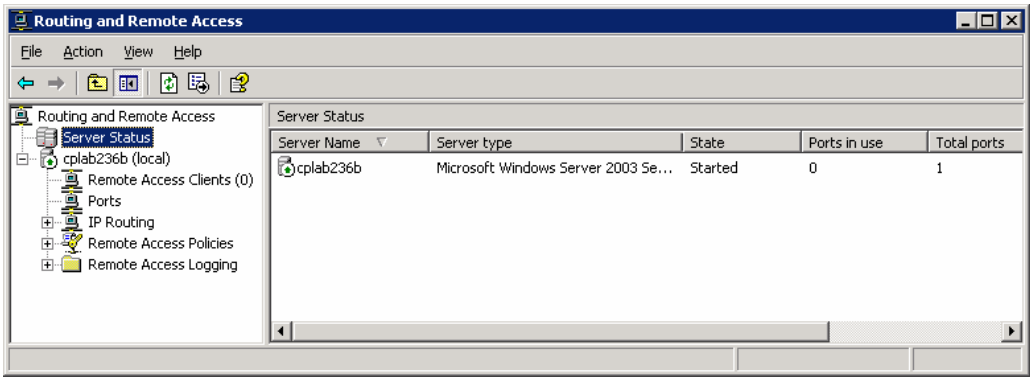
1. Click Start > Settings > Network Connections
2. Right-click on the NIC Card and click on Properties. The CLAN (or ELAN) Properties screen will appear.
3. Click on the Configure... Button. The Network Connection screen will appear.
4. Select the Advance Tab
5. For 703t and 1002rp:
    a. Highlight Link Speed and Duplex then select the required setting from the Value Drop-down Box on the right. Default value is Auto-Detect.
6. For 201i:
    a. Highlight Duplex then select the required setting from the Value Drop-down Box on the right. Default value is Auto-Detect.
    b. Highlight Speed then select the required setting from the Value Drop-down Box on the right. Default value is Auto-Detect.

8.1.10 RAS connection to server unstable and drops

When the client makes a connection to a CallPilot server through a modem and RRAS, the connection appears unstable and finally drops. The connection is negotiated, modem to modem, and then RRAS on the server side assigns temporary IP addresses to both the client and the server. From the client, when the server is pinged using the assigned IP address (typically 192.168.0.1), mostly timeouts occur but some packets are successful. After a short period of time, the connection may drop. Impacted are any remote applications including Microsoft RDC, pcAnywhere, CallPilot Manager, Application Builder, etc. Refer to CR # Q01070343.

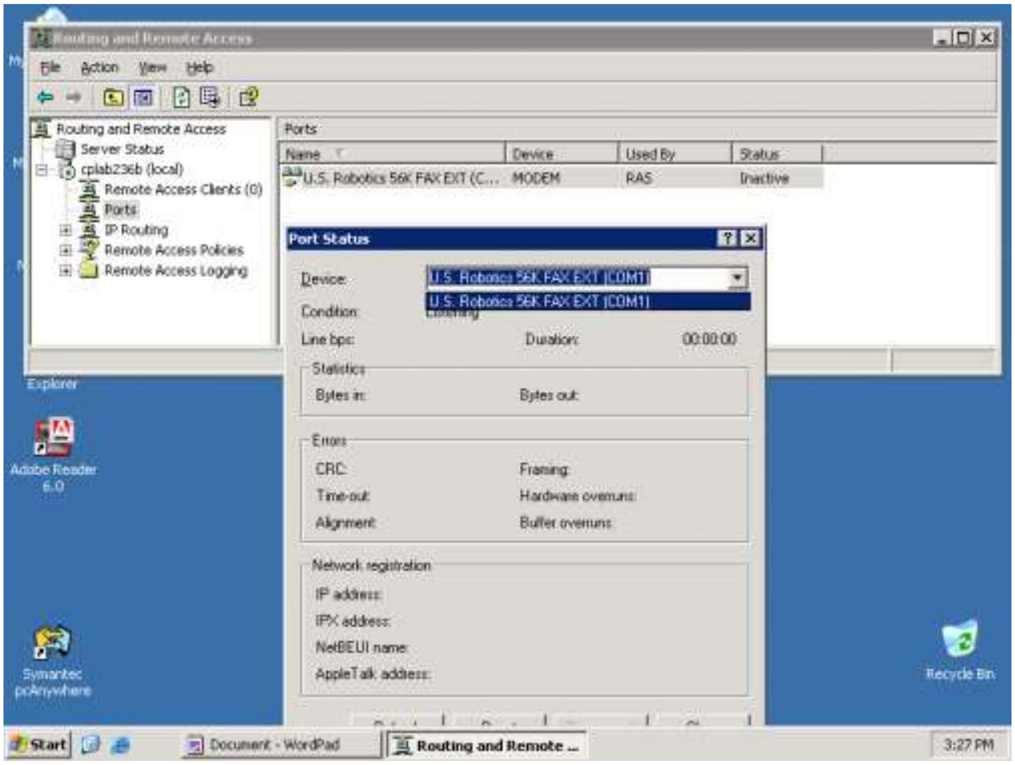
Workaround: The problem described above may occur if two (2) modem devices are configured for COM1, the one that was actually connected (US Robotics 33.6 FAX Ext. PnP) and one not connected to the system, in CallPilot's case the Standard 33600 Modem. Because of this, it instability is caused by the incorrect driver being used for the US Robotics modem.

To verify if two devices are connected to COM1, look into the Routing and Remote Access application (Start > Programs > Administrative Tools > Routing and Remote Access). Under Server Status there should only be one (1) total port. In the case of this failure, there may be two (2) or more.



Server Name	Server type	State	Ports in use	Total ports
cplab236b	Microsoft Windows Server 2003 Se...	Started	0	1

Under Ports, select the modem and then Status. There should be only one device listed in the drop down list box (U.S. Robotics 56K FAX EXT (COM1), but in this case there was also the Standard 33600 modem.



Name	Device	Used By	Status
U.S. Robotics 56K FAX EXT (C...	MODEM	RAS	Inactive

Device: U.S. Robotics 56K FAX EXT (COM1)
U.S. Robotics 56K FAX EXT (COM1)
Condition:
Line bps:
Duration: 00:00:00

The only method of removing the incorrect modem (e.g. Standard 33600 modem) from RRAS is to remove it from the system.

The method used is to remove all modems from the system under Windows Device Manager, and then scan for new devices with only the correct modem connected to COM1. The Standard 33600 modem was now removed from the system; RRAS only contained the U.S. Robotics 56K FAX modem and automatically finds the correct driver.

8.1.11 ELAN Disables After RDC /console Connection Over RRAS IP Address

When connected to CallPilot system using RDC over a RAS connection, the AML may occasionally restart with the following events appearing in the system log:

```
6/7/2005 2:31:35 PM AML_TSP Information 42802 N/A CALLPILOT The AML Link is up
6/7/2005 2:31:34 PM AML_TSP Information Startup 42804 N/A CALLPILOT TSP has started, CDN call model is
    in effect
6/7/2005 2:31:02 PM AML_TSP Warning 42800 N/A CALLPILOT The AML Link is down.
    Cinit::DoStartStepSocket – Socket re-started to Host address 137.135.128.253
6/7/2005 2:30:56 PM AML_TSP Error Information 42800 N/A CALLPILOT The AML Link is down. %1
```

Additional symptoms may include:

- CallPilot manager slow to respond
- Ring-No-Answer (RNA)
- ELAN bounce
- System locks up due to High CPU

Note: It has been observed that once the RDC session is terminated the system recovers on its own. This issue was investigated through wi00683871, wi00675682, wi00675684, and wi00679179 and identified as a Microsoft 2003 RDC issue that Microsoft does not plan to address.

Workaround: The following options for remote access on the 201i are:

1. Use pcAnywhere, LogMeIn Rescue, VNC, or WebEx

2. Use RDC with the following recommendations. Note that these recommendations decrease (but not eliminate) the likelihood of a service interruption with RDC.

    - Local resources – The local resources tab controls if your disks and printers are available once you connect. In order to copy files you must have disk drives checked. You should NOT have printers checked. With printers checked – any printer installed on your machine, even network printers will be installed on the CallPilot Server. There is no benefit to having your printers available and the extra bandwidth/processing power consumed should be avoided. Please review your RDC connections and make sure printers are unchecked.

    - The recommended way to connect – In the majority of cases you will want to connect by specifying the computer name or IP address and /console – e.g. 192.168.0.1 /console – Using /console gives you full control of the server and logs off the user at the console. If you do not specify /console – you are in a virtual session and do not have full control of the machine. In a virtual session there are numerous tools/programs that will not function properly.

Note: These recommendations decrease (but not eliminate) the likelihood of a service interruption with RDC.

8.1.12 List Tape Procedure with SLR32 and SLR50 Tape Drives

When performing a backup and restore in the same session (i.e. a system upgrade) on either an SLR32 or SLR50, a list tape performed before the restore will take an additional hour if the following two steps are not executed. This problem is due to an incompatibility with the Windows Server 2003 operating system and the use of aging tape drivers.

Workaround: Once the backup has been complete remove the tape cartridge. Do not reinsert the tape cartridge until the CallPilot server has been rebooted. If the tape is inserted before the reboot takes place, the problem will still occur.

8.1.13 List tape operation is too slow

If a system backup is completed and tape is left in drive, then List Tape operation (from CallPilot Manager or CallPilot Backup and Restore tool) may take a long time to respond.

Workaround: Eject the tape from the drive after system backup is completed, then re-insert tape.

8.1.14 Remote Desktop Connection requires root console for CallPilot tools

When logged in through RDC you must be connected to root console to use CallPilot tools.

Workaround: This requires running the 'shadow 0' command when connecting when you connect using "Method-1/Private" or "Method-2/Shared'. Reference Product Bulletin
P-2005-0226-Global / CallPilot 201i / Using RDC

8.1.15 Fax cover pages contain garbled characters if Mandarin Chinese (PRC) installed

CallPilot offers using a standard fax cover page when sending faxes to Express Fax messages SDN or using Desktop Fax feature. If this option is enabled and CallPilot has an Eastern Asian (e.g. Mandarin Chinese – PRC) language installed as a primary language, then standard fields on the fax cover page may contain corrupted characters. Refer to CR Q01943268 and wi00683758.

Workaround: A workaround exists for Mandarin Chinese (PRC) fax templates.

1. Contact Avaya support and obtain two files associated to CR #Q01943268
    a. Install_readme.txt
    b. Patch_Q01943268.exe.pdf
2. Download both files, place "patch_Q01943268.exe.pdf" on the target CallPilot server, and rename it to "patch_Q01943268.exe".
3. Follow the "install_readme.txt" to install corrected templates on the CallPilot server.
4. Once templates are installed, go to "Start > Settings > Control Panel > Regional and Language Options > Languages tab.
5. Select "Install files for East Asian languages". Click OK on the pop-up window. Click Apply.
6. This will prompt for Windows Server 2003 disk to be inserted in order to find i386 folder. Instead, point it to C:\e386 folder which exists on each CallPilot server.
7. Once installation is over **do not reboot CallPilot** but wait for a minute because 'Windows File Protection' window may appear. This is normal. Just click 'Cancel' and the 'Yes' in order to save all changes.
8. Reboot CallPilot.

8.1.16 Fax quality over IP

When sending\receiving CallPilot faxes using standard VoIP protocols such as SIP, RTP, T.38, etc. it is required that a certain network Quality of Service (QOS) is maintained to ensure faxes are delivered complete, and successfully. Jitter, Round trip delay, and packet loss can all have an adverse effect on faxes.

Workaround: Avaya recommends no greater than 40ms of jitter, and less than 10% packet loss otherwise faxing may result in missing content, non-readable pages, and log errors.

8.1.17 Potential Ring-No-Answer condition on 201i with Voice/Fax on same DSP

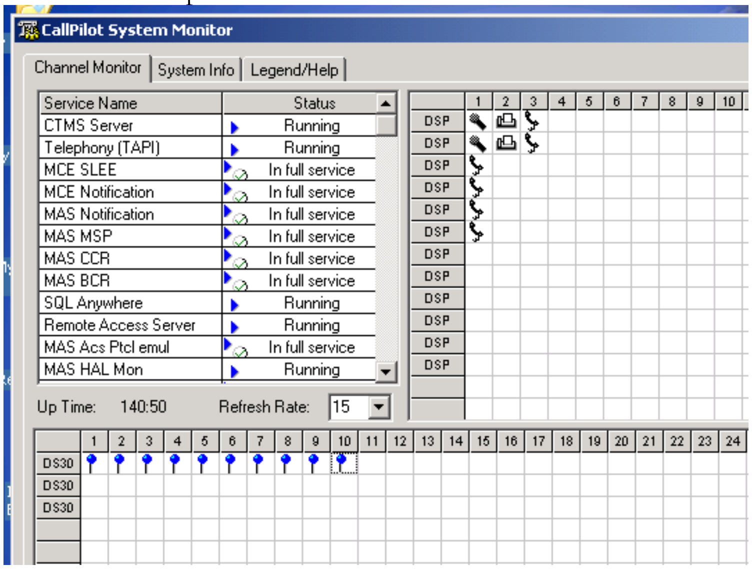
CallPilot 201i IPE servers may sometimes encounters RNA when Voice and Fax exist on the same DSP Card.

Event 38007 usually indicates the system is degrading and will eventually give RNA.
Event 38007 is usually followed by SLEE Events 58207 and 55213. Refer to wi00684695.

Example of the event:
d/mm/yy hh:mm:ss xM Ngen Error Major 38007 N/A UKMSLCP01 Event from
Signal Processing Component[DSP-1-1] : A DSP has not replied to an Audit command [Line= 1529, File=x:\mpcx.vob\mpcx\nblls\src\nblls_dll\lls_core\nblls_main.cpp].

Workaround:
As a workaround to prevent the DSPs from getting into the RNA state, on 201i IPE only, Voice and Fax DSP Resources should be re-arranged to separate DSP. Therefore after the workaround is implemented no single DSP Card must contain both Voice and Fax Ports.

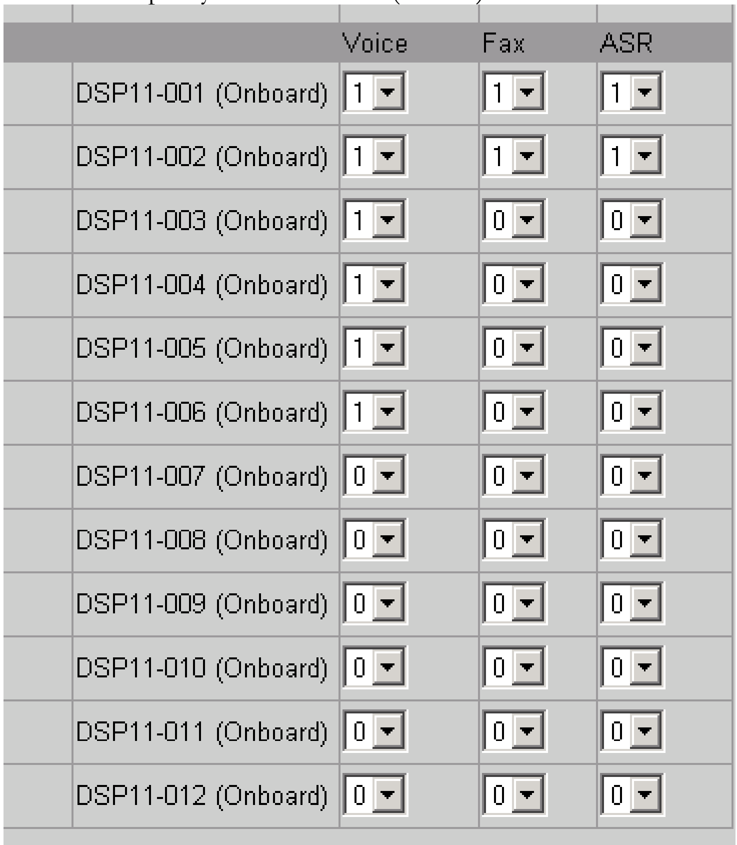
BEFORE example:



Service Name	Status
CTMS Server	Running
Telephony (TAPI)	Running
MCE SLEE	In full service
MCE Notification	In full service
MAS Notification	In full service
MAS MSP	In full service
MAS CCR	In full service
MAS BCR	In full service
SQL Anywhere	Running
Remote Access Server	Running
MAS Acs Ptcl emul	In full service
MAS HAL Mon	Running

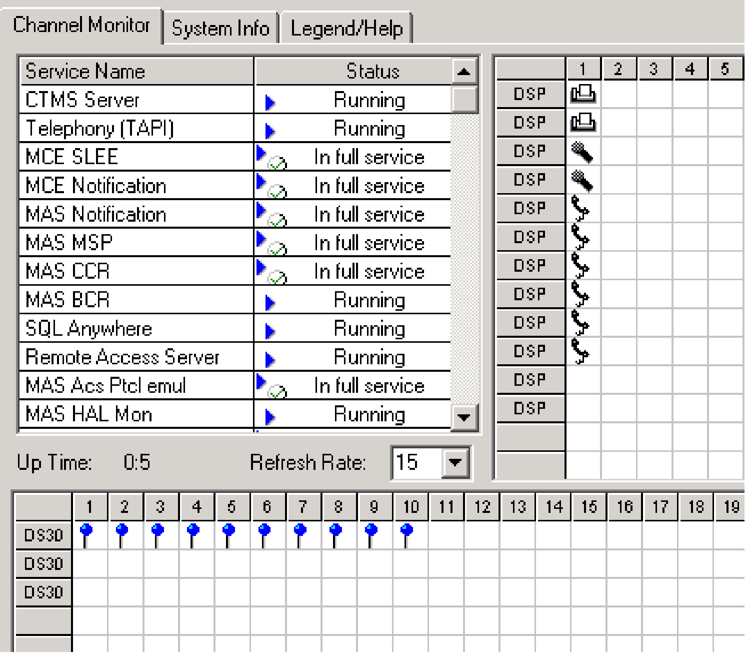
Up Time: 140:50 Refresh Rate: 15

Before example system allocation (default):



	Voice	Fax	ASR
DSP11-001 (Onboard)	1	1	1
DSP11-002 (Onboard)	1	1	1
DSP11-003 (Onboard)	1	0	0
DSP11-004 (Onboard)	1	0	0
DSP11-005 (Onboard)	1	0	0
DSP11-006 (Onboard)	1	0	0
DSP11-007 (Onboard)	0	0	0
DSP11-008 (Onboard)	0	0	0
DSP11-009 (Onboard)	0	0	0
DSP11-010 (Onboard)	0	0	0
DSP11-011 (Onboard)	0	0	0
DSP11-012 (Onboard)	0	0	0

AFTER example:



Service Name	Status
CTMS Server	Running
Telephony (TAPI)	Running
MCE SLEE	In full service
MCE Notification	In full service
MAS Notification	In full service
MAS MSP	In full service
MAS CCR	In full service
MAS BCR	Running
SQL Anywhere	Running
Remote Access Server	Running
MAS Acs Ptcl emul	In full service
MAS HAL Mon	Running

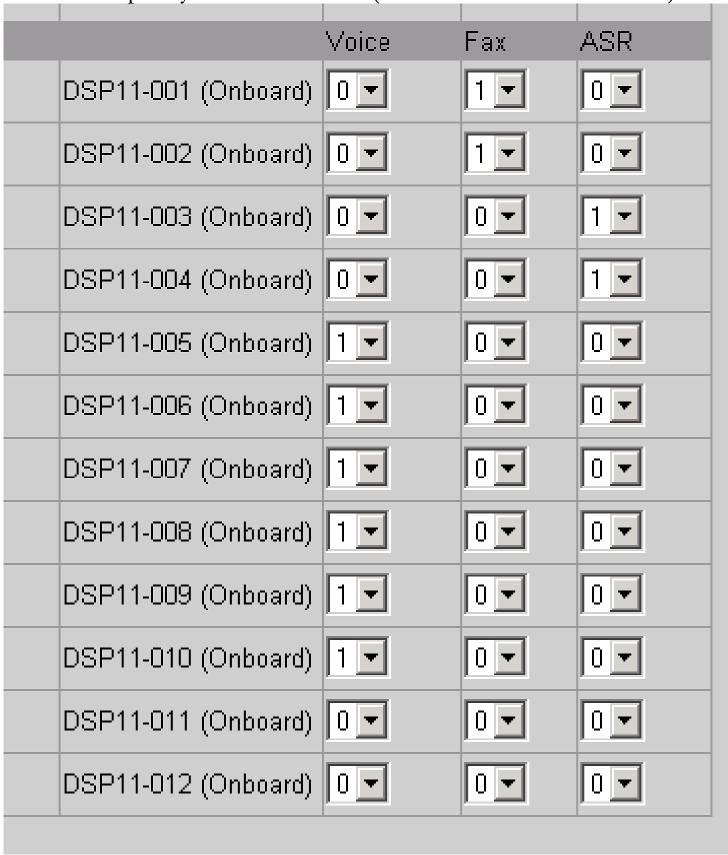
Up Time: 0:5

Refresh Rate: 15

	1	2	3	4	5
DSP	📠				
DSP	📠				
DSP	🎤				
DSP	🎤				
DSP	☎				
DSP	☎				
DSP	☎				
DSP	☎				
DSP	☎				
DSP	☎				
DSP					
DSP					

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
DS30	📍	📍	📍	📍	📍	📍	📍	📍	📍	📍									
DS30																			
DS30																			

AFTER example system allocation (after manual re-allocation)



	Voice	Fax	ASR
DSP11-001 (Onboard)	0	1	0
DSP11-002 (Onboard)	0	1	0
DSP11-003 (Onboard)	0	0	1
DSP11-004 (Onboard)	0	0	1
DSP11-005 (Onboard)	1	0	0
DSP11-006 (Onboard)	1	0	0
DSP11-007 (Onboard)	1	0	0
DSP11-008 (Onboard)	1	0	0
DSP11-009 (Onboard)	1	0	0
DSP11-010 (Onboard)	1	0	0
DSP11-011 (Onboard)	0	0	0
DSP11-012 (Onboard)	0	0	0

8.1.18 RAID Firmware and Power Console update

The RAID subsystem requires the following two updates:

1. On 1002rp and 703t systems running CallPilot Releases 2.02 (2.01.27) or 2.5, you must update your RAID firmware, driver and power console *prior* to splitting the RAID and creating your backup. This will ensure that you can safely boot from the 2.02/2.5 side of the RAID in the event that you must back out of the 2.02/2.5 → 5.0 upgrade. If you attempt to run the Upgrade Wizard prior to updating your RAID software, it will warn you but allow you to continue to check your system. However, the Upgrade Wizard will not allow you to proceed to the upgrade portion of the wizard (i.e. create your backup) until you have updated the RAID software. The RAID software is available from the Enterprise Solutions PEP Library (ESPL) at https://support.avaya.com/espl using PEP ID “CP40_RAIDUpgrade” or by searching using the following parameters:
   - Product = CallPilot
   - Platform = Server
   - Release = 4.04.04
   - Status = Released

This update is detailed in bulletin “P-2005-0173-Global Introducing LSI Logic MegaRAID 320-2”

2) After the P-2005-0173 update described in #1 above has been completed an additional update to the RAID subsystem is required to update the firmware and Power Console application. To address an issue that could cause the RAID subsystem to go offline, it is required to update to RAID firmware version 1L51 and Power Console version 5.00n on all platforms except 1002rp Rackmount (which remain on RAID firmware version 1L37). Refer to CR # Q01836741. An associated change was made to the Upgrade Wizard. Once RAID firmware version 1L51 has been applied, Upgrade Wizard V34 (or later) must be used.

The RAID software is available from the Enterprise Solutions PEP Library (ESPL) at: https://support.avaya.com/espl using PEP ID “RAIDUpdate” or by searching using the following parameters:

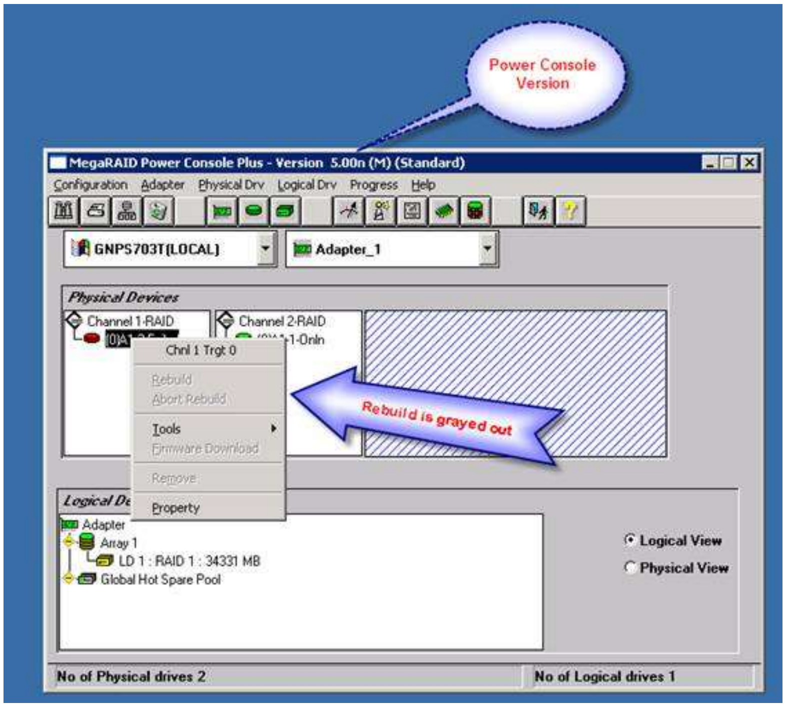
- Product = CallPilot
- Platform = Server
- Release = 5.00.41
- Status = Released

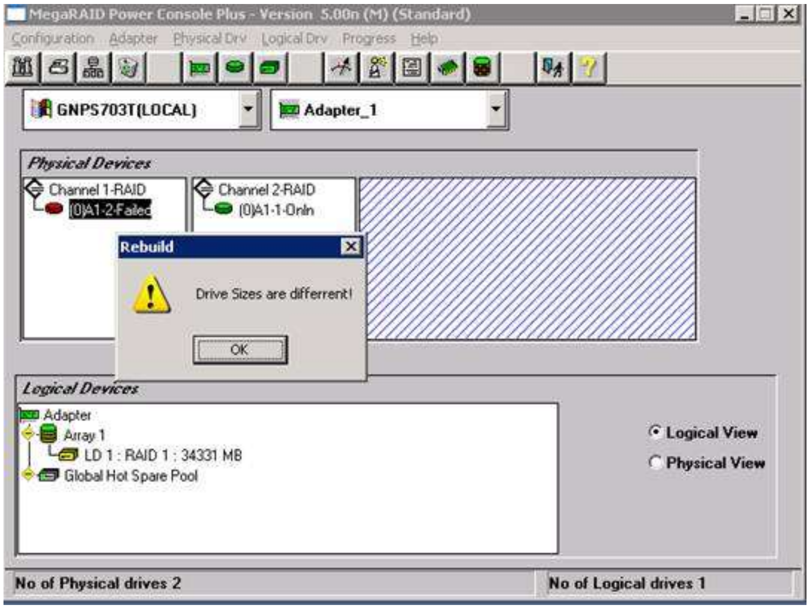
This update is detailed in bulletin “PAA-2008-0117-Global”

8.1.19 RAID “Rebuild Option” Grayed out

The option to rebuild is not available (grayed out) when right clicking on a physical drive under the Physical Devices section in the main screen. Attempts to rebuild through the Physical Drv pull down menu result in an error message indicating the drive sizes are different. Refer to wi00679819.

This problem only happens on systems using the LSI1600 RAID card and Mega RAID Power Console Plus GUI version 5.00n (CallPilot 1002rp and 703t servers using the LSI1600 RAID card).





Drive Sizes are differrent!

WORKAROUND:

Rebuild the drives through the MegaRAID BIOS utility.

These procedures assume that the RAID system is configured per the recommendations in the NTP documentation. If you are unsure on how to proceed, please contact your next level of support.

Drive pair settings for 1002rp server

LED No	ID	Channel-1	LED No	ID	Channel-2
0	0	A01-01	3	0	A01-02
1	1	A02-01	4	1	A02-02
2	2	A03-01	5	2	A03-02

Procedure for 1002rp servers:

1) Reboot the CallPilot server.
2) Press Ctrl+M while the server is booting, when the LSI Logic Corp BIOS message appears and the Ctrl+M option flashes.
3) Wait for the RAID configuration utility to open.
4) Select Objects and then Physical Drive.
5) Wait for scanning to complete.
6) Select the first drive on the channel containing the failed drives that need to be rebuilt. If the drives on Channel 1 are failed, the first drive will be A01-01. If the drives on Channel 2 are failed, the first drive will be A01-02).
7) Press enter on the drive.
8) Move the cursor to Rebuild and press enter.
9) Select Yes to confirm.
10) Wait for the rebuild process to complete.
11) Repeat steps 7 – 10 on the second and third drives on the channel containing the failed drives (If the drives are on Channel 1, A02-01 and A03-01. If the drives are on Channel 2, A02-02 and A03-02)
12) Press Esc to return to the Objects menu.
13) Press Esc to return to the Management menu.
14) Press Esc to exit the RAID configuration utility.
15) Click Yes to confirm that you want to exit the RAID configuration utility and press Enter.
16) Press Ctrl+Alt+Delete to reboot the server.

Drive pair settings for 703t sever

ID	Channel-1	ID	Channel-2
0	A01-01	1	A01-02

Procedure for 703t servers:

1) Reboot the CallPilot server.
2) Press Ctrl+M while the server is booting, when the LSI Logic Corp BIOS message appears and the Ctrll+M option flashes.
3) Wait for the RAID configuration utility to open.
4) Select Objects and then Physical Drive.
5) Wait for scanning to complete.
6) Select the first drive on the channel containing the failed drive that needs to be rebuilt. If the drive on Channel 1 is failed, the drive will be A01-01. If the drive on Channel 2 is failed, the drive will be A01-02).

7) Press enter on the drive.
8) Move the cursor to Rebuild and press enter.
9) Select Yes to confirm.
10) Wait for the rebuild process to complete.
11) Press Esc to return to the Objects menu.
12) Press Esc to return to the Management menu.
13) Press Esc to exit the RAID configuration utility.
14) Click Yes to confirm that you want to exit the RAID configuration utility and press Enter.
15) Press Ctrl+Alt+Delete to reboot the server.

Avaya Technology teams are aware of the issue and are working towards a solution with the OEM vendor that supplies the RAID card for CallPilot servers.

The MegaRAID Power Console Plus GUI upgrade is still recommended per PAA-2008-0117-Global CallPilot RAID Subsystem – Power Console Software and Firmware Updates Required, due to the issues with the MegaRAID Power Console Plus GUI version 5.00i software documented in that bulletin.

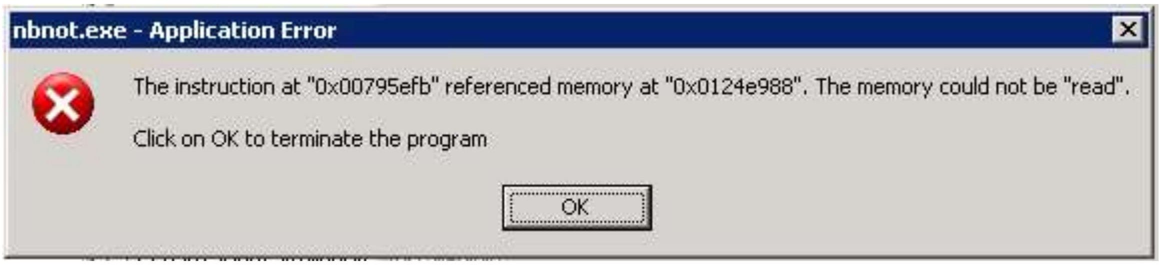
8.1.20 PowerConsole and Anti-Virus interactions

Risk of system degradation (server lock-up with Blue Screen of Death) exists if accessing Power Console during the same time a Symantec anti-virus full-system scan is being performed. If experienced, a full server reboot is required for recovery.

Workaround: To avoid this potential problem scenario, only access Power Console during times when Symantec anti-virus scans are not being performed.

8.1.21 Application Error pop-up when re-installing CallPilot Manager

Infrequently, after uninstalling CallPilot Manager, during the re-install, the following Application Error window may appear. Refer to wi01186868.



nbnot.exe - Application Error

The instruction at "0x00795efb" referenced memory at "0x0124e988". The memory could not be "read".

Click on OK to terminate the program

Workaround: There is no impact of this pop-up window. Click OK to resume re-installation of CallPilot Manager and other PEP updates.

8.2 CallPilot Manager

8.2.1 Unable to log into CallPilot Manager due to unknown password

Access to CallPilot Manager requires the user to have an Administration account/password.
If the default Administration Password (mailbox "000000", password "124578") has been changed and forgotten or misplaced, a utility exists with CallPilot 5.1 "Support Tools" for resetting it to the default.

Note: This utility requires access to CallPilot "Support Tools". If you do not have the password, you'll need to engage your next level of support to obtain it or for them to assist with the reset procedure outlined below.

Workaround: Use the following procedure to reset the default administrator password.

1. Log in to "Distributor" Support Tools on the CallPilot Server
   Start → Programs → CallPilot → System Utilities → Support Tools
2. From the main menu, select (9) Database Utilities
3. From the Database Utilities menu, select (3) Database API Utility
4. At the CI> prompt, type "resetadminpwd" and press <Enter>
5. At the CI> prompt, type "quit". This will close the API Utility
6. In the main menu, press <Enter>, and then select (1) to exit.

The default Administration mailbox "000000" password will be reset to "124578"

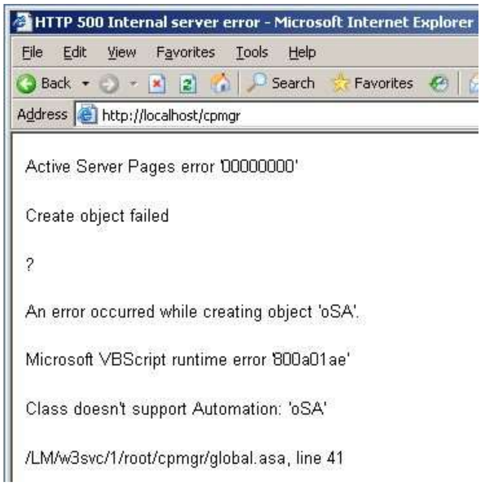
8.2.2 Change Windows password via ConfigWiz when original password in unknown

In CallPilot 5.1, only the Administrator Windows account exists and is used to manage the CallPilot server. If the Administrator password is forgotten or unknown, there is no supported method to recover the password. The server must be re-imaged and recovered using a recent system backup.

Please ensure that you store your Windows Administrator password in a safe place for later reference.

8.2.3 Cannot Launch CPMgr from standalone Windows Server 2003 Web Server configured as Domain Controller

When CallPilot Manager/Reporter is installed on Windows Server 2003 configured as a Domain Controller, CallPilot Manager cannot be launched. Refer to wi00934238. See below for error message and workaround.



Active Server Pages error '00000000'

Create object failed

?

An error occurred while creating object 'oSA'.

Microsoft VBScript runtime error '800a01ae'

Class doesn't support Automation: 'oSA'

/LM/w3svc/1/root/cpmgr/global.asa, line 41

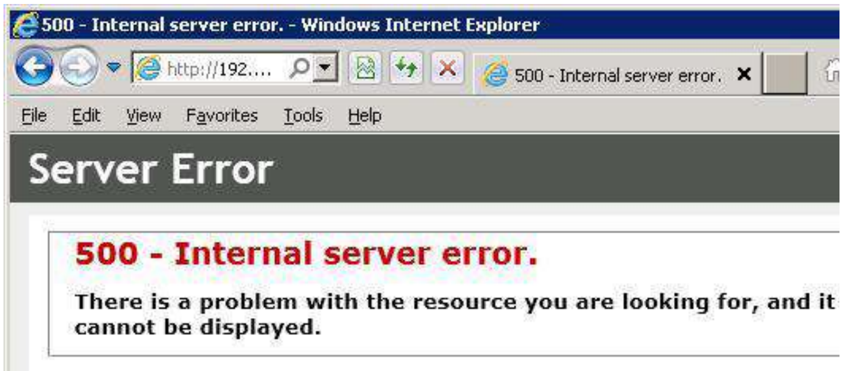
Workaround: To avoid the issue, additional DCOM permissions must be set manually.
Please do not remove any user from the group list

HOW TO CONFIGURE WINDOWS SERVER 2003 WITH ACTIVE DIRECTORY FOR CALLPILOT REPORTER:

1. Open Start->Administrative Tools->Component Service.
2. On the left pane of Component Services go to Component Services->Computers->My Computer ->DCOM Config->CallPilot Reporter.
3. Open Security tab in CallPilot Reporter properties.
4. Under Launch and Activation Permissions click Customize, and then click edit.
5. Add NETWORK group with Remote Activation and Local Activation permissions granted.
6. Add NETWORK SERVICE group with Local Launch and Local Activation permission granted.
7. Click Ok.
8. Open Start->Run… ->launch gpedit.msc
9. On the left pane of Group Policy Object Editor go to Computer Configuration -> Windows Settings -> Security Settings ->Local Policies -> Security Options
10. On the right pane click on DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax.
11. In DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax window click on Edit Security… button.
12. Add NETWORK group with Remote Activation and Local Activation permissions granted.
13. Click Ok. Click Ok.
14. Reboot.

8.2.4 Cannot Launch CPMgr from standalone freshly imaged Windows Server 2008 with error 500

When CallPilot Manager/Reporter is installed on freshly imaged Windows Server 2008, CallPilot Manager cannot be launched with error 500 - Internal server error. Refer to wi01121523. See below for error message and solution.


500 - Internal server error. - Windows Internet Explorer
http://192....
500 - Internal server error.
File
Edit
View
Favorites
Tools
Help

Server Error

500 - Internal server error.

There is a problem with the resource you are looking for, and it cannot be displayed.

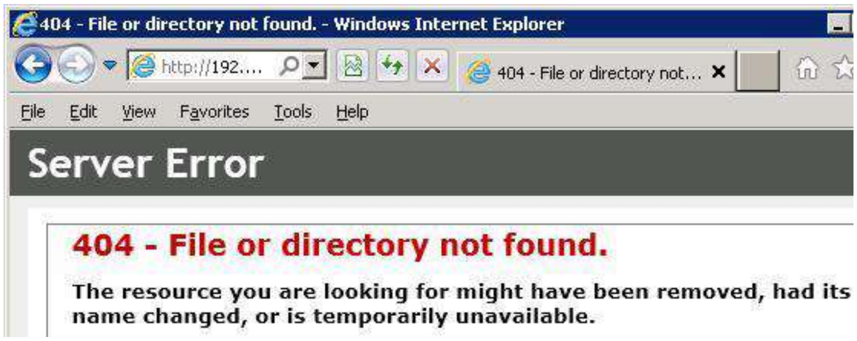
Solution: To avoid the issue, ASP.Net Role Service must be installed.

HOW TO CONFIGURE WINDOWS SERVER 2008 FOR CALLPILOT REPORTER:

1. Open Start->Administrative Tools->Server Manager.
2. On the left pane of Server Manager select Roles.
3. Scroll the right pane to Web Server (IIS) and expand it if required.
4. Click Add Role Services.
5. Check ASP.NET and click Next.
6. Click Install.
7. Click Close.
8. Reboot.

8.2.5 Cannot Launch CPMgr from standalone freshly imaged Windows Server 2008 with error 404

When CallPilot Manager/Reporter is installed on freshly imaged Windows Server 2008, CallPilot Manager cannot be launched with error 404 - File or directory not found. Refer to wi01121523. See below for error message and solution.


404 - File or directory not found. - Windows Internet Explorer
http://192....
404 - File or directory not...
File
Edit
View
Favorites
Tools
Help

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

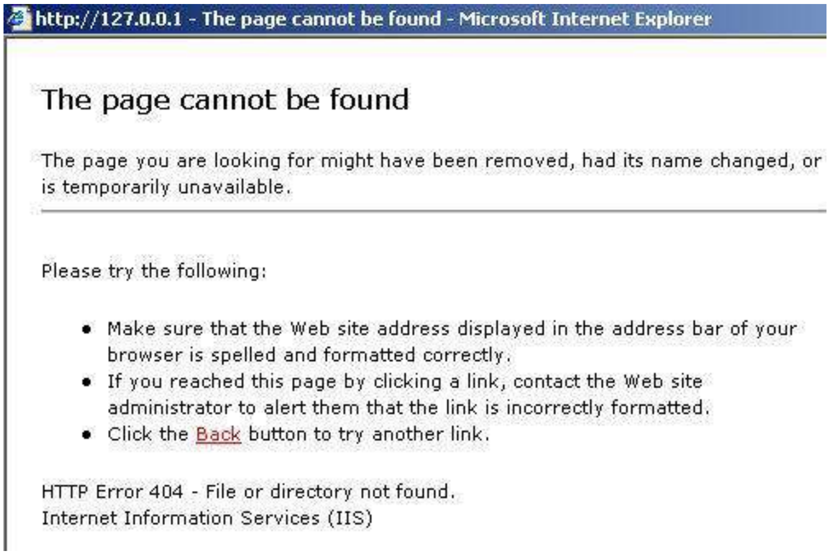
Solution: To avoid the issue, ASP Role Service must be installed.

HOW TO CONFIGURE WINDOWS SERVER 2008 FOR CALLPILOT REPORTER:

1. Open Start->Administrative Tools->Server Manager.
2. On the left pane of Server Manager select Roles.
3. Scroll the right pane to Web Server (IIS) and expand it if required.
4. Click Add Role Services.
5. Check ASP and click Next.
6. Click Install.
7. Click Close.
8. Reboot.

8.2.6 Cannot run reports from standalone freshly imaged Windows Server 2003 with error 404

When CallPilot Manager/Reporter is installed on freshly imaged Windows Server 2003, Reports cannot be launched with error 404 - File or directory not found. Refer to wi01121523. See below for error message and solution.



http://127.0.0.1 - The page cannot be found - Microsoft Internet Explorer

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the Back button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

Solution: To avoid the issue, .Net Framework v2.0 or higher must be installed.

Follow this link to get .Net framework v2.0:
http://www.microsoft.com/en-us/download/details.aspx?id=1639

8.3 Event Monitor/Viewer

8.3.1 Events 2, 3, 4, 8, and 9 appear in System Event logs

When accessing the CallPilot server via a Remote Desktop, Events 2, 3, 4, 8, and 9 may appear in the System Event log. These events reference LAN printers even though no print action was performed by the user. Refer to CR # Q00943668.

Workaround: Discontinue using Remote Desktop or simply disregard the events. They have no known impact to CallPilot.

8.4 High Availability

8.4.1 Isolation recovery failed on the HA systems

Description: HA prototype failed to come back to the normal state after all Ethernet links resumed during the isolation test, unless the AutoStart Backbone and Agent were restarted manually. We need to know how to automatically start the AutoStart Agent on the previously isolated server after all Ethernet links are recovered. EMC team is looking into the issue and will provide the solution. Refer to wi00679171.

Workaround: Manually restart the AutoStart Backbone and Agent on the previously isolated server.

8.4.2 Both Heartbeat Down Issue

Description: The Standby server failed to come back to the normal state after both Heartbeat links were down for a short period of time. Refer to wi00679040.

Workaround: Manually restart AutoStart Backbone service.

8.4.3 Uninstall procedure for HA database PEP

PEPs which affect the database structure require a special uninstallation procedure. To uninstall database-affecting PEPs the following procedure should be used. This issue is documented under CR # Q01839795.

Note: To ensure that the pair of CallPilot servers functions correctly, both CallPilot servers must be running the same PEPs and Service Updates (SUs).

In this procedure, CP1 is the active server and CP2 is the standby server. This process causes the servers to go out of service while the PEPs are uninstalled.

Step 1: On CP1, do the following:

a. Launch the AutoStart Console.
b. Stop monitoring.
For more information, see "Disabling automatic failovers (stop monitoring)" (page 213).
c. Take the resource group offline (shutting down CallPilot). For more information, see "Taking the CallPilot resource group offline" (page 211).
d. Wait for the CallPilot resource group to go offline.
e. Attach the mirror drives (drive E and drive F) to CP1 so the disks can be accessed from CP1.

Note: Attaching and detaching drives can take a few minutes.
  i. In the AutoStart Console, select the **[AutoStart_Domain]**
  > Data Sources.
  ii. Right-click the drive you want to connect.
  iii. Select **Attach Data Source**.

f. Uninstall the PEPs.

Note: The PEP code is enhanced so that it starts any CallPilot services that it needs to have running (for example, the database).

g. Detach the data source.

h. In the AutoStart Console, select the **[AutoStart_Domain]**

> Data Sources.
  ii. Right-click the drive/data source.
  iii. Select **Detach Data Source**.

i. Restart the server (if required).

Note: Because the resource group is offline and monitoring is disabled, CallPilot does not automatically restart after the restart.

Step 2 On CP2, do the following:

a. Launch the AutoStart Console.

b. Attach the mirror drives (drive E and drive F) to CP2 so the disks can be accessed from CP2.

Note: Attaching and detaching drives can take a few minutes.
  i. In the AutoStart Console, select the **[AutoStart_Domain]**
  > Data Sources.
  ii. Right-click the drive you want to connect.
  iii. Select **Attach Data Source**.

c. Uninstall the PEPs.

Note: The PEP code is enhanced so that it starts any CallPilot services that it needs to have running (for example, the database).

d. Restart the server (if required).

Note: Because the resource group is offline and monitoring is disabled, CallPilot does not automatically restart after the restart.

Step 3 On CP1, do the following:

a. Launch the AutoStart Console.

b. Start monitoring (to enable automatic failovers). For more information, see “Enabling automatic failovers (start monitoring)” (page 214).

c. Bring the resource group online (starting up CallPilot). For more information, see “Bringing the CallPilot resource group online” (page 209).

8.5 Meridian 1 Systems

STI link 32 ports with TNs from two different MGate cards results in no voice

Each STI link must be programmed individually with the matching MGate card on all 32 channels. Refer to NTP NN44200-302 and wi00684600, wi00678427, and wi00678457 for further details.

8.6 T1 Systems

8.6.1 T1: Delay in call transfer/thru-dial/call sender with CallPilot T1 integration.

A 4-9 seconds silent delay will be experienced when using any of the transfer, thru-dial or call sender functions before ring back is heard. Refer to wi00678811, wi00678853, and wi00684641.

The debounce value may need to be set to 25 or higher. If the default value of 13 is configured, call transfer, thru-dial and call sender functions may not function in some implementations.

8.6.2 Call Sender from Desktop or My CallPilot fails

Using Line-side T1/SMDI integration, Call Sender from Desktop Messaging or My CallPilot may fail. Refer to wi00678443.

Workaround: To correct this issue, ensure the switch is equipped with Line-side T1 cards (NT5D11) release 5 or later.

8.7 201i Platform and distorted fax

In very rare instances it has been seen where faxes are received with a blurry line or light distortion. This issue is limited to the CallPilot 201i server platform and has only been seen with excessive fax usage in certain configurations. The CallPilot 201i platform was never intended to serve as a fax server, and for that reason this limitation is being documented for supported configurations. If this issue is seen, the corrective action is to limit the number of active fax sessions to two (2) by configuring no more than two fax channels. Refer to CR # Q01811937.

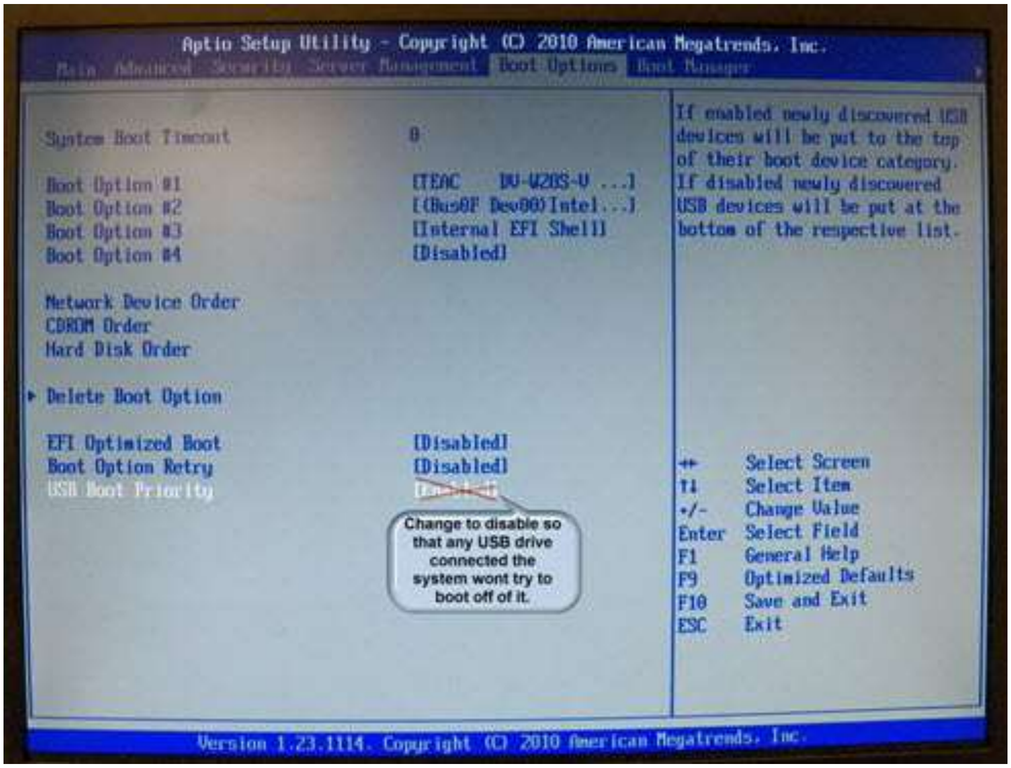
8.8 600r Platform

The CallPilot NTRH40AA MPB96 PCI DSP board is not physically compatible with the 600r due to insufficient mechanical clearances. For the 600r you must use the RoHS complaint NTRH40AAE5 or NTRH40CAE5 (CAT-5E) variants. Surplus NTRH40AA PCI cards can safely be used with the 1005r, 703t or 1002rp.

8.9 600r/1006r Platform fails to boot/reboot with RDX drive attached.

Tandberg RDX is an external hard disk drive used for backup/restore of CallPilot data/messages. With a cartridge inserted, the unit powered on, and plugged into the CallPilot 1006r rackmount system, upon a startup, or restart, the system may attempt to boot from the RDX drive device and fail. This issue has been duplicated with BIOS version 50 and BIOS version 54 (upgraded via firmware upgrade package release 1.3). Refer to wi00892262.

Workaround: To allow the system to boot properly with the RDX drive attached, powered-on, and with a cartridge inserted, disable “USB boot priority” option in the BIOS under the “Boot Options” tab.



```
Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
Main  Advanced  Security  Server Management  Boot Options  Boot Manager

System Boot Timeout            0                    If enabled newly discovered USB
                                                    devices will be put to the top
Boot Option #1                 [TEAC    DV-W28S-V ...]  of their boot device category.
Boot Option #2                 [(Bus0F Dev00)Intel...]  If disabled newly discovered
Boot Option #3                 [Internal EFI Shell]     USB devices will be put at the
Boot Option #4                 [Disabled]               bottom of the respective list.

Network Device Order
CDROM Order
Hard Disk Order

▸ Delete Boot Option

EFI Optimized Boot             [Disabled]
Boot Option Retry              [Disabled]           ↔      Select Screen
USB Boot Priority              [Enabled]            ↑↓     Select Item
                                                    +/-    Change Value
                                                    Enter  Select Field
                                                    F1     General Help
                                                    F9     Optimized Defaults
                                                    F10    Save and Exit
                                                    ESC    Exit

Version 1.23.1114. Copyright (C) 2010 American Megatrends, Inc.
```

Change to disable so that any USB drive connected the system wont try to boot off of it.

8.10 My CallPilot & Desktop Messaging

8.10.1 Outlook – Custom Form Could Not Be Opened

When opening a new message within desktop messaging, a pop-up error is generated stating "The custom form could not be opened. Outlook will use an outlook from instead".

It appears the CallPilot Add-in (nmdcext.dll) is becoming disabled during the upgrade of desktop messaging. Neither a reboot nor re-installing the desktop messaging application fixes the issue.

The only way that you can listen to the message is via the 'vbk' format. Refer to wi0686158.

This error condition may be the result of Office ending unexpectedly and at the same moment, some add-in component was in a loading state. After restarting Office, the component becomes disabled which may cause other add-ins to also be disabled.

Workaround: Manually re-enable disabled Office add-in components as follows:

<u>Outlook 2003:</u>

1. In MS Outlook navigate to Tools->Options menu.
2. Select Other tab, then click Advanced Options… button.
3. In Advanced Options window click COM Add-Ins… button.
4. Select and enable the CallPilot Extensions add-in.

<u>Outlook 2007:</u>

1. In MS Outlook navigate to Help->Disabled Items… menu.
2. Select and enable the CallPilot add-in (nmdcext.dll).

8.10.2 Server lookup mode in CallPilot Address Book on Novell GroupWise 8.0

If Desktop Messaging installation is configured to use server lookup mode in CallPilot Address Book there might be some issues with Novell GroupWise address book application (called "addrbook.exe"). GroupWise address book application is having trouble with filtering addresses, while Desktop is fully functional in this mode and can dynamically filter addresses when composing CallPilot message. This behavior should be addressed in future versions of Desktop Messaging.

8.10.3 My CallPilot access from CallPilot server

My CallPilot can be accessed from the Internet Explorer browser on a CallPilot server. In some cases, when security PEPs are installed on a CallPilot server, tightening of browser security settings may result in pop-up warnings or could cause some Internet web sites to not function properly. For example, a pop-up warning may appear stating: "A script is accessing some software (an Active X Control) on this page which has been marked safe for scripting. Do you want to allow this?"

No workaround to be provided, in order to prevent CallPilot server exposure to malware and attacks. Avaya's recommendation and design intent is to not access My CallPilot directly from the CallPilot server. Refer to wi00888207.

8.10.4 Display incorrect sender when sending message to email address with Microsoft Outlook”

When sending a CallPilot message to the e-mail address (not a CallPilot recipient) the sender of the message will be the Exchange account. Outlook sends a message via Exchange server if a recipient is an e-mail. This behavior is as design intent. For more details refer to wi00891375.

8.10.5 Outlook 2010 / CallPilot Desktop messages do not show up in combined Outlook inbox.

When using “Deliver to e-mail inbox” with Outlook’s “Cached Exchange Mode” turned off, CallPilot messages do not show up in combined view. Refer to wi00933551.

Workaround: Manually turn on Cached Exchange mode as per instructions below.

8.10.6 Outlook 2010 / New CallPilot messages addressed to the CallPilot address remain in the Outbox and Exchange Server generates non-delivery report.

When composing messages with Outlook’s “Cached Exchange Mode” turned off, CallPilot messages remain in outbox and result in NDN report. Refer to wi00893872.

Workaround: Manually turn on the Cached Exchange mode as follows
1. In Microsoft Outlook 2010, navigate to File > Info > Account Settings
2. Select Microsoft Exchange account and click “Change”.
3. Turn on checkbox “Use Cached Exchanged Mode”
4. Click “Next”.
5. Warning “The operation you selected will not complete until you quit and restart Microsoft Outlook” appears. Click “OK”.
6. Click “Finish”.
7. Close Account Settings
8. Restart Outlook

8.10.7 Unable to attach files to message when sending to multiple users

A My CallPilot user cannot attach Text, VBK, WAV, or TIF files to a new CallPilot message if more than 40 recipients are included in the TO address list of the message. Internet Explorer and Mozilla Firefox show error pages with the following description "The request filtering module is configured to deny a request where the query string is too long.". This is a result of the URL max query string restriction. If the query string length is larger than the restriction, URL requests will not be run and the above mentioned error page will be shown. This restriction may be set on IIS 7.0 and later. Internet Explorer 8 and older IE versions have the query string length hard-coded. Refer to wi01040070.

Workaround: Workarounds to the issue exist, depending on Windows OS and browser in used.

For Windows Server 2008 (x32 or x64), with Mozilla Firefox or Internet Explorer 9

1. Launch CMD prompt
2. Enter "CD C:\Windows\System32\inetsrv"
3. Enter "appcmd list config /section:requestFiltering –text:requestLimits.maxQueryString"
    a. Results: shows the current value of maxQueryString configured on your PC
4. If the maxQueryString value is displayed, execute the following command:
    a. "appcmd set config /section:requestFiltering /requestLimits.maxQueryString:4096"

For Windows Server 2008 (x32 or x64) with Internet Explorer 8 or older

1. Install Internet Exploer 9 on your Windows server and run commands from workaround above or decrease number of recipients because IE 8.0 has the hard-coded max query string restriction that cannot be bypassed.

For Windows Server 2003 with Internet Explorer 8 or older

1. Decrease the number of recipients in the TO list of the new message, splitting the intended recipients up into smaller lists in multiple outgoing messages

8.11 Upgrade Wizard

Upgrade Wizard did not detect incorrect BIOS version

NTP NN44200-400 states that the BIOS version for a 1002rp platform must be NNCXUA07. However the Upgrade Wizard does not check confirm whether NNCXUA07 BIOS is installed. If the BIOS is not updated to NNCXUA07 then the user may experience product activation issue. Refer to wi00685685.

Workaround: Follow either the documented procedure in the 1002rp maintenance and diagnostics NTP, or use the Windows COA provided with the system from the factory to activate.

8.12 Meridian Mail to CallPilot migration

8.12.1 Restriction Permission Lists may cause migration errors

When Migrating from Meridian Mail to CallPilot, it is imperative that RPL names do not conflict; otherwise the migration process may skip data. Refer to wi00682921.

Workaround: Prior to migration, either rename all existing CallPilot RPLs, or simply delete them from the CallPilot database. This ensures proper mailbox Class-of-Service/RPL orientation.

8.13 CPTrace Utility on Windows 2008

8.13.1 CPTrace utility doesn’t show messages from My CallPilot

When the CPTrace utility is launched on Windows 2008 Server SP2, in the trace windows there are no trace messages from MyCP. The root cause of this problem is that IIS is a service that can't exchange data with the desktop application on Windows 2008 Server. The solution is to design a new tracing mechanism. Tracing to file is still available but it's necessary to set privileges for Network Service to write into a trace file. Refer to wi01001822.

Workaround: To set necessary privileges, perform the following steps:

1. Open directory which you have chosen for keeping trace log file
2. Right click on it and choose “Properties”
3. Choose the pane “Security” and click the “Add” button
4. In the textbox type “Internet Service” and click the “OK” button
5. Choose “Network Service” in “Group or user names” and allow “Full Control”. Click the “OK” button

9 PEP/Service Update application overview

Performance Enhancement Packages (PEPs) and Service Updates (SUs) are software fixes or updates that enhance CallPilot features and operation. CallPilot PEPs generally deliver individual fixes while Service Updates contain more comprehensive updates. As PEPs/SUs are delivered periodically, it's recommended the Enterprise Solutions PEP Library (ESPL) website be checked regularly to ensure the latest updates are applied.

The most recent PEPs for CallPilot 5.1 can be found on the Enterprise Solutions PEP Library (ESPL) website at: http://support.avaya.com/espl

Note: If you are new to the ESPL website, you will need to register for a user ID/password. Please apply on-line or contact your Avaya Channel Partner Account Manager.

9.1 PEP Numbering Format

The PEP numbering format for server PEPs includes supplemental information for which Service Update they apply to using format: CPRRRSSSXYYZ:

Where:

RRR:	Software Release (e.g. 5.01, 5.00, 4.00, 3.00, 2.50, 2.02)
SSS:	The required SU level required to apply the PEP Example: (S01 = Service Update 01)
X:	The type of PEP: (G)eneral, (R)estricted, (L)imited, or (D)iagnostic.
YY:	The PEP number (01-99).
Z:	The component that is being PEPed / updated: (S)erver, (C)allPilot Manager, (A)pplication Builder, (M)y CallPilot, or (D)esktop client.

The CallPilot server is the only component that will have small PEPs. Other components may have PEPs released, but the PEP will really contain an updated version of the software package. The following list summarizes the different components and how they are PEPed:

CallPilot Server:	PEPS
CallPilot Manager:	PEPs/Software update
Reporter:	Packaged as part of CallPilot Manager software update
My CallPilot:	Software update
Desktop:	Software update

9.2 CallPilot 5.1 Service Update 3 (SU03) and Individual PEPs

At the time of this printing, the following CallPilot 5.1 SU03 PEPs are available for download.

9.2.1 CallPilot 5.1 Service Update 3 (SU03) Individual PEPs

The following Individual PEPs are available for download.

PEP number	Description
CP0501SU003S	CallPilot 5.1 Service Update 3 (SU003) server component.
CP501S03G05C	CallPilot Manager (05.01.03.03) required for use with CallPilot 5.1 and installed on CallPilot server and/or optional stand-alone web server for Reporter.
CP501S03G04A	Application Builder (05.01.03.02): Required for use with CallPilot 5.1; installed on client PC.
CPSECPEP017S	CallPilot Server Security Update #17 (includes Microsoft hotfixes up to MS14-051 and other OS/Application security hardening. Requires CPSECPEPSP2S.
CPSECPEPSP2S_V02	Microsoft Windows 2003 Server/Service Pack 2 (SP2). Not applicable to 202i and 1006r servers as is pre-installed/included in server image.
CP501_Desktop_05.01.03.03	Desktop PC client version 5.01.03.03: includes support for the latest groupware and OS environments
CP501_MyCallPilot_05.01.03.03	CallPilot server and/or web-server component: My CallPilot version 5.01.03.03 – includes support for latest OS and browser versions
ABExplorer_v2	CallPilot Application Builder Explorer Utility (v2); installed on Windows PC.
CallPilot_MIBs	MIBs for SNMP traps for alarms/events
CP1006r_FIRMWARE_1.3	1006r servers only: Firmware Upgrade Package Release 1.3
CP201_POHS	201i IPE only: Disk Power-On Hours Utility for release 3.0 and later systems
CP500_HighAvailability	1005r or 1006r H/A servers only: latest EMC software (EMC5.3.3 (SP2) and EMC_Hotfix)
CP501_UpgradeWizard_v0302	Enhanced Upgrade Wizard (version 05.01.03.02) for use when upgrading to 5.1 from release 5.0/4.0/3.0 (any SU), 2.5/SU02, or 2.02/SU04.
CPDRVPEP001S	CallPilot server component: Driver for US Robotics USR5637 56K USB Faxmodem.
CPDRVPEP002S	CallPilot server component: Driver for Tandberg RDX External USB drive to ensure ejects button functions correctly.

PEP number	Description
EMC5.3.3	1005r or 1006r H/A servers only: EMC AutoStart 5.3 Service Pack 3 (SP3)
RAIDUpdate_1L51_v2	703t and 1005r servers only: RAID firmware update

9.2.2 CallPilot Service Update 3 (SU03S) Content

CR/wi #	Description
wi00677842	Fax Autoprinting is disabling itself - no user notification
wi00686228	Event 55211 for DN unsubscribed is cryptic with poor help
wi01050995	Restore from the Backup Restore Tool does not perform a database update
wi01067471	CallPilot Notification service crashed when RN number was disabled because of a RPL conflict
wi01100408	MFR fails and disables due to message from Anonymous
wi01100419	Callpilot 5.0 MTA service memory leak
wi01102210	Out-of-office notifications received from MS Exchange server 2010 are empty
wi01102211	Read receipts received from MS Exchange server 2010 are truncated
wi01102342	CallPilot archive fails some users with an 41813 ldap 60605 error but no indication of why
wi01104034	Calls to or from CallPilot Fax fail up to half of the tries
wi01104047	CallPilot Inactive User Report shows duplicate records about user’s mailbox logins
wi01104902	Audio player is not displayed fully on IE10
wi01106992	GR Sync Status Monitor is incorrect
wi01107111	CallPilot slowly degrades to intermitant RNA with event 38016 hint Memory Corruption
wi01108595	Calls to CallPilot Fax fail intermittently with the hint "Resource timeout" while sending over trunk
wi01114376	Corrupt voice form message causes hang up when accessing through transcription service
wi01117684	CallPilot successful FAXs create Event 58208 Hint=Operation Abort
wi01125443	Release of CallPilot server should be updated to 05.01.03
wi01125750	CallPilot Reporter Administrator Action Report shows 127.0.0.1 for all changes until a Messaging change is done
wi01127772	CP 5.1 PEP upgrade failure with duplicate Class of Service
wi01132228	CallPilot Backup\Restore Enhancement: Fax Autoprinting is disabling itself - no user notification
wi01132876	Desktop Messaging enhancement Fax Autoprinting is disabling itself - no user notification
wi01138964	CallPilot T1/SMDI green lollipops and PLO with CP5.1 SU02 PEPs
wi01140215	Memory could not be written to after applying 5.1 SU02
wi01141141	Enhancement: Eliminate Duplicate COS check utility need for blue password
wi01144318	Enhancement: Voice Forms, option to disable "Recording Stopped" prompt
wi01144591	CallPilot GR syncronization fail with event code 36207
wi01144596	GR synchronization stops working on large systems when used across WAN
wi01150927	MTA service terminates with GR and MFR
wi01154285	HA implementation fails at bringing LOAD DN process online with
wi01155727	GR synchronization fails to synchronize users with events 54103, 54104
wi01157652	COS check utility enhancement: additional features are needed.
wi01162408	CallPilot HA stops answering calls with all DSPs busy event 57303

CR/wi #	Description
wi01166404	Callpilot Reporter keeps dropping conection, every few days. Getting 41001 and 41003 events.
wi01171431	[CallPilot Reporter] Unread messages showed incorrectly in Inactive User Report after User login then logout its My Callpilot.
wi01172259	Callpilot Manager version is showed incorrect after running setup wizard
wi01175843	Customer receiving “Undeliverable Messages” two days after a GR Pair failure/recovery only happens when using proxie/exhange
wi01178690	IMA error pops up once after fix in PEP G14S was applied on platform 1005r or newer.

9.2.3 CallPilot Manager PEP CP501S03G05C Content

The following fixes and enhancements are addressed with CP501S03G05C.

CR/wi #	Description
wi00677859	Reporter: notice about free space termination on the Reporter local disk
wi01091241	Auto-Add needs e-mail address field to complement password change service
wi01091242	Advanced Search doesn't offer Password Change Service e-mail field
wi01102347	Index and word search boxes are not displayed in CP Manager online help
wi01107254	Unable to dial new Directory Entry User until re-saved
wi01107947	Prechecks are needed in the Reporter's installer to avoid problems during deployment
wi01110120	Copyright version on CP Password Change Service page should be updated as CP Manager page
wi01112017	Sorting fields is displayed incorrect on Web StandAlone Win server 2008 32 bits
wi01113328	There is no content in CP Reporter help pop-up notes in IE8, IE9, IE10
wi01113612	No content in Reporter online Help using IE10
wi01115680	Copyright is not showed when accessing Online CallPilot document from Application builder
wi01119076	No content in CallPilot Manager online Help using IE10
wi01121523	Insufficient documentation to install Reporter on freshly imaged 2008 server
wi01125437	CallPilot Reporter sorting option usage causes report to fail
wi01125440	CallPilot Reporter cannot be backed up on a 2008 web server
wi01126253	CallPilot 5.1 Reporter reports do not give scroll bar to view report
wi01131416	CallPilot Manager Enhancement: Fax Autoprinting is disabling itself - no user notification
wi01138721	CallPilot Reporter sort of Mutimedia Building Block Summary Report is out of order when more than one day pulled.
wi01144318	Enhancement: Voice Forms, option to disable "Recording Stopped" prompt
wi01165367	CPMgr Security - Cross-Site Scripting vulnerability
wi01167246	CPMgr Security - Link Injection / Cross-Site Request Forgery

9.2.4 CallPilot Application Builder PEP CP501S03G04A Content

The following fixes and enhancements are addressed with CP501S03G04A.

CR/wi #	Description
wi01144693	Need to update calendar year in the footer of Application Builder 05.01.03.01

9.2.5 CallPilot Server Security PEPs

CallPilot 5.0 factory-images contain all applicable Windows security updates through Jan 16, 2007 excluding 202i and 1006r which contain additional updates including Service Pack 2 (SP2) given their introductions post 5.0's GA.

For a list of additional individual Microsoft Security Updates (hotfixes) that apply to CallPilot 5.1 servers running the Windows Server 2003 Operating System, refer to Product Bulletin "CallPilot Server Security Update-<year>" or Product Security Advisory Alerts.

To apply Microsoft Security Updates, use Start > Windows Update.

At the time of writing, the following security PEP is available.

PEP number	Description
CPSECPEP017S	CallPilot Server Security Update w/ Microsoft hotfixes up to MS14-051/additional enhancements.

The following fixes are addressed with CPSECPEP017S.

CR/wi #	Description
Q01367189	Excessive TCP Keep-Alive LAN traffic with Desktop Messaging
Q01449531	DMI view update sets CPservices to disabled after installing PEP CP202SEC004S
Q01617017	MSI-Format support for CallPilot
Q01637569	Receiving numerous event 59 and 32 in system log
Q01638452	CP40404SU04S failed to install on a 703t with CallPilot 4.0 GA
Q01781913	PEP CPSECPEP009S crashes CallPilot
Q01783689	Need Windows Administrator account to launch CallPilot Manager Homepage
Q01806764	PEP CPSECPEP010S makes many main functions of CallPilot work incorrectly
Q01807104	CPSECPEP010S – Some securities are not added as expectation
Q01807140	Some enhancement securities are not configured properly
Q01807505	Users can configure proxy setting in IE
Q01807989	Service "Help And Support (helpsvc)" is not configured as document mentioned
Q01819279	Some registries are not added as expected
Q01819385	Cannot login to Support Tools on CP sever joined to Domain
Q01830619	Wrong service name in readme.txt (TrkSrv)
Q01853690	Cannot map drive for network backup after installing CPSECPEP010S
Q01973128	CPSECPEP011S fails to install on 202i
Q01980200	Application popup after installation of CPSECPEP011S
Q02094497	Microsoft Base Security Analyzer fails after installing CPSECPEP011S
Q02116123	DCOM errors EVENT ID: 10020
Q02133709	DCOM Events10005 is generated after each reboot
wi00858836	New Security PEP needed for CallPilot servers
wi01055706	Unable to install CPSECPEP015S unless previous SU has been installed
wi01102418	New Security PEP needed for CallPilot

9.2.6 CPSECPEPSP2S

The package contains Windows Server 2003/Service Pack 2 (SP2) to be installed on CallPilot server release 3.0, 4.0, 5.0 and 5.1 servers. It is a prerequisite to install PEP CPDSKPEP001S prior to installing CPSECPEPSP2S on 201i, 703t and 1002rp platforms running release 3.0, 4.0, or 5.0.

Note: CPSECPEPSP2s is not applicable to 202i IPE or 1006r Rackmount servers. The system image comes pre-installed with this update.

Note: There is no additional fix content in CPSECPEPSP2S_V02 against CPSECPEPSP2S v. 1.4 (the previous released version of CPSECPEPSP2S). There were changes only in readme file:

- We added clarification about CR Q01886717
- we documented how do deal with situations where there was insufficient C: drive space

If you have CPSECPEPSP2S already installed on your system no action is required.

Note: At the time of this printing, this package has been certified for installation on CP5 HA systems. It has not been certified on CallPilot 4 JITC Hardened systems.

9.3 CallPilot 5.1 Service Update Carried-forward solutions

9.3.1 CallPilot Server Content

The following solutions and enhancements were provided in a previous SU or PEP:

CR/wi #	Description
wi00936992	Some data is lost in the HA_Unloaded_Tables during SU installation
wi00979005	CallPilot Reporter Administrator Report Client IP and description fields not correct
wi00979372	CallPilot GR pair with 54104 and 40261 events
wi00981881	Unable login to GR mailbox after remote notification call
wi00986305	CallPilot server enhancement: Ability to customize the Remote Text Notification messages
wi00986319	CallPilot server enhancement: MFR - need option to choose WAV message encoding type
wi00995517	CallPilot 1002rp T1/SMDI is running High CPU and Memory
wi01012336	CallPilot degrades to ring no answer with SLEE and BCR errors following SU10 / SU11 update
wi01012340	GR message sync fails if message sub-type is "Unknown"
wi01018511	Event 54103 errors are being generated when deleting local users if VPIM networking is configured
wi01018832	Mailboxes fail to sync to GR Partner if Comments field contains a <carriage return> in user mailbox
wi01026988	Callpilot GR users are not updated with 54104 events
wi01030125	CallPilot 5.1 install on CPHA - SQL errors returned during install
wi01034129	Sending a message to more than 5740 recipients fails
wi01034147	CallPilot Access port give dead air after 2nd set of voice segments
wi01037551	Service Update README; Adjust RAID verbiage from optional
wi01042949	CallPilot GR with many 54104 events followed by system degradation

CR/wi #	Description
wi01047047	CallPilot Ports go to green lollipop and do not release
wi01047713	CallPilotWebServiceCert certificate expired
wi01051014	CallPilotWebServiceCert certificate expired
wi01052013	Event 54103 intermittently generates when a Call Answering message is replicated to the GR server
wi01052097	System Monitor does not show PEP lineup after upgrade to 5.1 PEPs
wi01054662	Error code on windows server 2008 when adding voice form backup
wi01056891	Server generating event 36209 and 36211
wi01058522	CallPilot 1002rp T1/SMDI Higher memory usage after SU10 installed
wi01059654	First RN disabled by entering invalid number
wi01066121	CallPilot Manager Channel Monitor shows blank screen
wi01074303	Intermittent no response on ACCESS integrated calls
wi01076040	CallPilot GR 54104 Events with Time stamp error when a message is not being updated
wi01076045	CallPilot Manager backup and archives fail with Event 59201 RC=4
wi01076051	CallPilot answers and then drops with 56004 and 56008 SLEE errors
wi01079428	CallPilot Reporter report for inactive users has some dates that do not match CallPilot
wi01080818	CPU optimization to improve system peformance
wi01082023	Event 54825 doesn't provide sufficient details to understand root cause
wi01082058	Event 36785 doesn't provide sufficient details to understand root cause
wi01082065	Event 54119 doesn't provide sufficient details to understand root cause
wi01086523	CallPilot GR Network Diagnostic test Fail
wi01087617	Event 54119 needs to be changed
wi01090851	No Prompt IDs listed under System Prompt Customization

9.3.2 CallPilot Manager Content

The following solutions and enhancements were provided in a previous version of CallPilot Manager

CR/wi #	Description
DE2425	CallPilot Reporter for Windows 2008 Web Server
wi00686150	Password Change Service localization
wi00686226	Ability to customize the Remote Text Notification messages for CallPilot Manager
wi00923830	CallPilot Manager - User Search doesn't provide MFR search
wi00929785	CallPilot Manager cannot be installed/uninstalled properly on Windows Server 2008
wi00971880	RPL property is not shown via Firefox (2.0) browser
wi00972233	CallPilot Copyright version is wrong
wi00979038	RPL restriction popup when changing Mailbox Class and adding RN target DN
wi00986217	Data is not aligned properly in a report when exported to Excel format
wi00986319	CallPilot server enhancement: MFR - need option to choose WAV message encoding type
wi00986326	CallPilot Manager enhancement: MFR - need option to choose WAV message encoding type
wi00986326	CallPilot Manager enhancement: MFR - need option to choose WAV message encoding type
wi00989071	When user selects to view both graph and tab reports only graph reports appear
wi00989076	Error is displayed trying to view some reports
wi00989134	IIS worker process eats up memory when high traffic is ran on Reporter server
wi01002005	Admin Action report is not displayed correctly with CallPilot Manager installed on web standalone Windows server 2003 and 2008
wi01009301	Update latest NTP into online help
wi01013719	Cannot create more than 32 CDNs in Configuration Wizard
wi01015406	Unable run Reports when CallPilot Reporter installed on Windows Server 2008
wi01015613	There is no content from Online Help Using IE9 with CallPilot Reporter

CR/wi #	Description
wi01016119	Delete CDNs operation works incorrectly in Configuration Wizard
wi01016201	The progress bar doesn't show during Auto Delete progress
wi01018043	Unable open Synchronization Task log on windows 2008_32 bits
wi01019939	CallPilot Administrator can't enable/disable RN on Mailbox User Detail page
wi01039979	Unable to install Reporter on Windows Server 2008 R2 Standard 64Bits SP1
wi01040769	MFR is disabled automatically on CallPilot Manager
wi01041376	CallPilot Reporter data exceeding OM limit settings
wi01041664	This WI is to submit updated CallPilot Manager On-line help
wi01042905	Unable adding new report and viewing properties report on Windows 2008
wi01042938	Unable to install Reporter on Windows Server 2008 R2 Standard 64Bits SP1
wi01042942	This WI is to submit updated CallPilot Manager On-line help
wi01047636	RPL property is not shown via FireFox (2.0) browser
wi01048226	Copyright version on 'CallPilot Password Change Service' should be updated
wi01050121	MFR is disabled automatically on CP Manager
wi01052183	CallPilot Reporter data exceeding OM limit settings
wi01053344	Copyright version on 'CallPilot Password Change Service' should be updated
wi01053483	Application Builder link does not show up in CallPilot Manager if Flight Recorder is not in default mode
wi01053485	Application Builder link does not show up in CallPilot Manager if Flight Recorder is not in default mode
wi01056168	Update latest NTP into online help
wi01059459	Error display instead of content in Online HELP using other language with Google Chrome and Safari Web Browser
wi01061928	CallPilot Reporter purge operation could not be planned or executed properly
wi01061955	Reports cannot be exported as scheduled
wi01061964	No content in CallPilot Manager Online HELP with Google Chrome and Safari Web Browser
wi01063089	Scheduled reports are not saved on disk on Windows Server 2008 R2
wi01079375	CallPilot Reporter reports fails to show graph reports with logon failed error
wi01083639	When using Sorting options through CallPilot Reporter, some reports do not display and popup error is generated
wi01088489	Reports are saved and generated with incorrect format
wi01092741	Unable to dial new Directory Entry User until re-saved
wi01092836	CallPilot Manager/Reporter - need compatibility with Windows8 IE 10
wi01097451	Need to update CallPilot online documentation for CP5.1 SU02
wi01101285	Index and word search boxes are not displayed in CP Manager online help
wi01103547	No content in Reporter online Help using IE10
wi01106044	Copyright version on CP Password Change Service page should be updated as CP Manager page
wi01109410	Sorting fields is displayed incorrect on Web StandAlone Win server 2008 32 bits
wi01123617	CallPilot Reporter sorting option usage causes report to fail
wi01124053	CallPilot Reporter cannot be backed up on a 2008 web server

9.3.3 CallPilot AppBuilder Content

The following solutions and enhancements were addressed in a previous version of AppliationBuilder.

CR/wi #	Description
wi00974327	Warning box should be corrected
wi00986319	CallPilot server enhancement: MFR - need option to choose WAV message encoding type
wi01090235	Need AppBuilder compatibility with Windows 8 OS environment

9.4 Documentation References

The following table provides a list of supplemental documentation, available at the time of this printing, which may be useful in support of CallPilot 5.1 servers.

Document Type	Document Number	Description
Product Bulletin	99067	CallPilot Unauthorized Hardware and Software
Product Bulletin	P-2005-0026-Global	CallPilot 3.0 and 201i IPE Platform – Using Microsoft Remote Desktop Connection
Product Bulletin	P-2008-0007-Global	CallPilot Support Tool – 201i Power-On Hours
Product Bulletin	P-2008-0153-Global	CallPilot MPB96 and MGate Updates
Product Bulletin	P-2008-0154-Global	CallPilot 201i IPE – Mertek KVM Cable
Product Bulletin	P-2008-0187-Global	CallPilot Spares Planning
Product Bulletin	P-2010-0012-Global	CallPilot Support Utility – AppBuilder Explorer
Product Bulletin		CallPilot Support for Anti-Virus Applications - 2013
Product Bulletin		CallPilot Server Security Update - 2013
Product Bulletin		CallPilot – Introducing Compatibility with VMWare
Product Bulletin		CallPilot 1006r Rackmount Hard Drive Replacement
Product Bulletin		CallPilot Business Partner Lab Support
Product Bulletin		CallPilot Desktop Messaging – Compatibility with Outlook 2010
Security Advisory		CallPilot Security Advisory – Symantec pcAnywhere
End of Sale Notice		CallPilot 1005r Rackmount Server
End of Sale Notice		CallPilot 600r Rackmount Server
End of Sale Notice		CallPilot End-of-Sale Notice
Sales/Marketing Bulletin	SM-2009-0053-Global	Introducing CallPilot 202i IPE Platform
Sales/Marketing Bulletin		Introducing CallPilot 1006r Rackmount Platform

Note: Many CallPilot NTPs are updated to reflect new content introduced in various Service Updates. It is recommended to download the current NTP "suite" and Offline Help to have the latest information in support of the new capabilities.

CallPilot product documentation (bulletins, NTPs, and Offline Help) are available through the Avaya Partner and/or Support Portal websites using these links:
Partner Portal: http://portal.avaya.com
Support Portal: http://support.avaya.com
CallPilot page: https://support.avaya.com/products/P0712/avaya-callpilot/

Appendix A CallPilot/Contact Center (SCCS) Integration

The following items should be reviewed to ensure proper integration between Symposium Call Center Server 4.2, Express 4.2, 5.0, or Contact Center 6.0 and 7.0 with CallPilot 5.1 for Voice Services. For High Availability integration with CCMS 6.0 or 7.0 only, refer to Appendix-F.

Software pre-requisites:

1. SCCS 4.2 with PEP NS040206SU07S or later
2. Express 4.2 with PEP CS040206SU08S or later
3. CallPilot 5.1/Service Update 2 (05.01.02)
4. Communication Server 1000 (release 5.0) or later with the following software packages:

		CallPilot	**Contact Center**
Pkg	**Description**	**X21**	**X21**
35	IMS – Integrated Message Service		*
40	Basic Automatic Call Distribution		*
41	ACDB (ACD Package B)	*	*
42	ACDC (ACD Package C)		*
43	LMAN – ACD Load Mgt Reports		*
45	ACDA (ACD Package A)		*
46	MWC – Message Waiting Center	*	
50	ACDD (ACD Package D)		*
77	CSL – Command Status Link	*	*
83	CDRQ – ACD CDR Queue Record		
98	DNIS – Dialed Number Identification Service		
111	TOF – ACD Timed Overflow Queuing		
114	AUXS – ACD Pkg D, Aux Security		*
153	X25AP – Application Module Link – AML	*	*
155	ACDNT – ACD Account Code		*
164	LAPW – Limited Access to Overlays	*	
175	NMS – Network Message Service	opt	
209	MLM – Meridian Link Modular Server		*
214	EAR – Enhanced ACD Routing	*	*
215	ECT – Enhanced Call Treatment	*	*
218	IVR – Hold in Queue for IVR	*	*
242	MULI – Multi-User Login	*	
243	Alarm Filtering	*	
247	Call-ID (for AML Applications)	*	*
254	Phantom TN	*	
296	MAT – Meridian Administration Tool	*	
311	NGCC – Avaya Symposium Call Center		*
324	NGen (MAS Connectivity)	*	*
364	NMCE (CallPilot)	*	

Note: The software packages listed above may be included as components in other X11/X21 packages. They are provided here individually for reference only. Refer to the ordering bulletins for each associated product for additional information.

Documentation available:

1. NTP NN44200-302: CallPilot 5.1 Installation and Configuration Guide, Part-3 Meridian 1 and CallPilot Server Configuration Guide
2. NTP NN44200-312: CallPilot 5.1 Installation and Configuration Guide, Part-3 Succession 1000 and CallPilot Service Configuration Guide
3. NTP NN44200-502: Meridian Mail to CallPilot Migration Utility Guide (if migrating voice prompts)
4. NTP 297-2183-931: Contact Center, CS1000/Meridian 1 Voice Processing Guide

Note: The Avaya Partner Portal website contains the above documents. Ensure the latest versions are utilized when integrating both solutions.

PBX configuration guidelines:

1. VAS/SECU setting for both CallPilot and SCCS ELAN/VAS-ID should YES
2. CallPilot agents segregated for SCCS support should be build w/ Class of Service: CLS-MMA and AST

Additional general notes:

1. **Recording Voice Prompts using telephone set requires Desktop Messaging License**
   The recording of Voice Prompts using a telephone set on CallPilot currently requires the Desktop Messaging application to be installed with appropriate licensing. Customers requiring this capability and not having Desktop Messaging should contact their Avaya prime to resolve this issue.

2. **Stop/Start of voice channels on CallPilot requires action on SCCS**
   If voice channels are stopped and re-started using CallPilot Manager (through Channel Monitor or Maintenance Admin), they will not resume voice processing until they have been de-acquired and re-acquired through the SCCS Client.

   Customers should avoid stopping and starting voice channels. If action is necessary, voice ports should be de-acquired and re-acquired through the SCCS Client Voice Ports window.

3. **GIVE CONTROLLED BROADCAST fails, returning only silence**
   The Give Controlled Broadcast script command does not currently operate properly when the CallPilot 5.1 and SCCS 4.2 systems are installed on the Communication Server 1000 switch running Release 5.0 or some systems using Superloops. Callers will hear silence rather than the specified voice segment if this script command is employed.

   Workaround: To resolve this issue, install PBX PEP MPLR18165 where appropriate.

4. **GIVE CONTROLLED BROADCAST not supported on CS1000E**
   The CS1000E uses IP to transmit media between Media Gateways and requires a DSP resource for all IP to TDM conversions. For the GIVE CONTROLLED BROADCAST feature it is necessary to provision a DSP in the MG containing CallPilot for each media path to be established to a caller terminating on a trunk in a different MG. Given the physical constraints

on the number of DSPs that may be provided in a MG, there are limitations on the use of this feature, effectively that it not be used when integrated with a CS1000E switch except when in Single-Chassis/Cabinet configurations. Technology is investigating this limitation and seeking to develop a solution.

For additional information reference Product bulletin P-2007-0179-Global Communication Server 1000 Release 5.0.

5. **ACCESS channels remain in an un-initialized state if CallPilot reboots before SCCS MLink service is started.**

   If the MLINK service is not up prior to the CallPilot system completing its initialization, the ACCESS channels will be put into an un-initialized state. Without manual intervention, the access channels will remain in an un-initialized state. From lab tests, SCCS takes approximately four (4) minutes to bring up the MLink service.

   Workaround: Defer the boot start time on CallPilot for five (5) minutes after SCCS starts its boot sequence. This can be done through the Windows Operating System setting:

   On the CallPilot server, from Control Panel → System → Startup/Shutdown. In “System Startup” set “Show list for” to 300 seconds. This will delay the CallPilot boot-up for five (5) minutes, giving SCCS time to boot first.

   What works with the workaround (5 minute delay to boot start of CallPilot):
   With both systems powered down (SCCS and CallPilot):
   a. Both CallPilot and SCCS can be powered up at the same time
   b. Both CallPilot and SCCS can survive an unattended power outage, assuming that both systems are attached to the same power source.

   What does not work with the workaround:
   a. During the first power-up of CallPilot, the workaround will not be applied. Therefore, cannot power up SCCS and CallPilot at the same time, for the first time.
   b. With a functional network (SCCS, CallPilot, and Meridian 1 / CS 1000)
   c. CallPilot rebooting in a 3-5 minute window prior to the SCCS rebooting.

6. **Migrating voice prompts from Meridian Mail requires additional steps**
   When migrating SCCS voice prompts, ensure the additional steps as outlined in NTP 44200-502 Meridian Mail to CallPilot Migration Utility Guide are completed prior to attempting to use those prompts within SCCS scripts.

7. **SCCS requires VOICE channels for integration**
   While CallPilot offers three channel types (Voice, Fax, and Speech Recognition), SCCS and CallPilot require dedicated voice channels for integration. As Voice channels utilize only a single MPU per channel, use of Voice channels is the most cost-effective resource, similar to that of the Meridian Mail "BASIC" and "FULL" service channels.

   To avoid conditions where no voice is presented, and to ensure the integration utilizes the most cost-effective resources, ensure that all channels that are to be used for SCCS voice services are dedicated voice channels.

8. **If VSM Request Failure events are seen on CCMS, the likely cause is one of the following**
   a. The port has not been added via CCMA
   b. The port has been configured as IVR, not ACCESS
   c. CallPilot has not successfully logged the port in on the CS 1000

9. **SCCS unable to acquire resources after improper shutdown/crash.**
   Symposium Call Center Service (SCCS) acquires devices such as TNs and ACD agent phonesets on the Meridian 1/Communication Server 1000. If the server crashes or is shutdown without running the shutdown utility, these devices will remain acquired. This can cause a number of problems including:

   1. If the SCCS has a problem such that it cannot de-acquire one or more devices, then these devices cannot be used by other applications until a switch SYSLOAD is performed.
   2. After the switch INIT, CDN count might be corrupted for an application link.

   In these (and possibly other) occasions, it is required to forcibly de-acquire resources from the Meridian 1/Communication Server 1000. Some commands have been developed as tools to perform these tasks, such as:
   - De-acquire all acquired devices of application over a specified ELAN link
   - De-acquire an acquired Agent TN
   - De-acquire an acquired Route of a Customer
   - De-acquire an acquired CDN
   - De-acquire an acquired ACDDN.

   The commands to de-acquire each of the resources are:
   From Overlay 48 (LD 48):
   1. De-acquire an acquired "AGENT":
      `DACR AGT <Loop> <Shelf> <Card> <Unit><CR>`
   2. De-acquire an acquired "ROUTE":
      `DACR RTE <Route#> <Customer#><CR>`
   3. De-acquire "ALL" acquired devices on a specified link:
      `DACR ALL <Link#><CR>`

From Overlay 23 (LD 23):

1. De-acquire an acquired "CDN”:
   REQ <DACR>
   TYPE <CDN>
   CUST <Customer#>
   CDN <XXXX>
2. De-acquire an acquired "ACDDN":
   REQ <DACR>
   TYPE <ACD>
   CUST <Customer#>
   ACDN <XXXX>

You can use overlays such as 10, 11, 20, 21, or 23 to confirm the action is carried out successfully on your device.

Appendix B CallPilot Performance and recommended Measurements

To avoid running into memory problems, the following measure are recommended to help with system performance:

1) It is recommended that no unneeded application programs are left running on the CallPilot server.
   - Quit out of Internet Explorer when you are done.
   - Quit out of Windows Explorer if you do not need it.
   - Log off the local console and properly log off (do not simply disconnect) from any Remote Desktop sessions when they are no longer required.
   - If Anti-virus software has been installed, double-check that the guidelines in product bulletin **"CallPilot Support for Anti-virus Applications"** have been followed completely. If AV configurations are being managed remotely (e.g. via McAfee ePolicy Orchestrator), please ensure that the configuration settings being applied to the CallPilot server properly conform to the bulletin.
   - Do not leave the Anti-Virus console running unnecessarily.
   - If Anti-virus software has not been installed, please take steps to ensure the CallPilot server has not become and will not be infected by a virus or other malicious software.
   - Ensure that any backups, AV scans or AV updates are performed at off-hours to minimize impact to system performance.

2) It is required that you do not:
   - Attempt any engineering-related configuration changes on the CallPilot server.
   - Add memory
   - Reconfigure the paging file.
   - Adjust partition sizes.

Appendix C CallPilot TCP/UDP Port Usage

The following TCP/UDP ports are required to be open on CallPilot server (ELAN & CLAN) and any server which communicates directly with CallPilot server (for example, standalone server running CallPilot Reporter).

L4 Protocol (TCP/UDP)	Port number or range	Description
TCP	20	FTP
TCP	21	FTP
TCP	25	SMTP
TCP	80	WWW
TCP	135	Location Service
UDP	135	Location Service
TCP	137	NETBIOS Name Service
UDP	137	NETBIOS Name Service
TCP	138	NETBIOS Datagram Service
TCP	139	NETBIOS Session Service
TCP	143	IMAP2
UDP	161	SNMP (if enabled)
UDP	162	SNMP-trap (if enabled)
TCP	389	LDAP
TCP	443	HTTP over SSL
TCP	465	SSMTP (secure SMTP)
TCP	636	LDAP over SSL
TCP	993	IMAP over SSL
TCP	1025	msdtc
TCP	1026	msdtc
TCP	1027	Microsoft Distribute COM Services
TCP	1028	Microsoft Distribute COM Services
TCP	1029	Dialogic CTMS
TCP	1030	Dialogic CTMS
TCP	1031	Dialogic CTMS
TCP	1032	Dialogic CTMS
TCP	1036	CallPilot Middleware Maintenance Service Provider
TCP	1037	CallPilot Call Channel Resource
TCP	1038	CallPilot Multimedia Resource
TCP	1039	CallPilot MCE Notification Service
TCP	1040	CallPilot MCE Notification Service
TCP	1041	CallPilot MCE Notification Service
TCP	1042	CallPilot MTA

L4 Protocol (TCP/UDP)	Port number or range	Description
TCP	1045	CallPilot Access Protocol
TCP	1046	CallPilot SLEE
TCP	1047	IIS
TCP	1048	IIS
TCP	1095	CallPilot Blue Call Router
TCP	1096	CallPilot Blue Call Router
TCP	1148	TAPI
TCP	1499	ODBC for Reporter Database
TCP	2019	Dialogic CTMS
TCP	2020	Dialogic CTMS
UDP	5000	CallPilot AOS DCOM (RPC)
TCP	5000	CallPilot AOS DCOM (RPC)
TCP	5631	pcAnywhere data
UDP	5632	pcAnywhere stat
TCP	7934	IIS
TCP	8000	Dialogic CTMS
TCP	10008	CallPilot Access Protocol
TCP	38037	msgsys Intel CBA-Message System
TCP	56325	CallPilot SLEE

Note: DCOMCNFG.exe must be used to statically assign DCOM endpoints to 5000. DCOMCNFG.exe is a part of the Windows operating system.

Appendix D CallPilot High Availability Troubleshooting Reference

The following sections provide troubleshooting information for CallPilot when configured in a High Availability (dual 1005r or 1006r servers) configuration.

Problem Types	Symptoms	What might be wrong	Where to check	How to fix
Bring CallPilot online	Failed at EnableAOS	Administrator's pwd was not changed.	Click EnableAOS on the Utility Processes list on AutoStart Console and then click the tab Settings.	Enter the right pwd on the Login Info section.
	Failed at LoadDN	Administrator's pwd was not changed, or the Directory path was changed wrongly.	Click LoadDN on the Utility Processes list on AutoStart Console and then click the tab Settings.	Check the Directory path first, and if nothing wrong there, enter the right pwd on the Login Info section.
	Failed at Managed ELAN IP	ELAN connection might be down.	Check the ELAN cable connection and ping the switch.	
	The resource group CallPilot became online after the manual failover and the system showed being able to accept calls, but calls failed to go through after dialed the CDN number.	Didn't put the right Managed ELAN IP into AutoStart_Configuration.ini.	E:\Nortel\HA	Add Managed ELAN IP into AutoStart_Configuration.ini.
Failovers	After failover, make calls but no voice prompt.	The DS30 cable connection to the CP server and the switch may fall off.	First make sure the DS30 cable connection to the CP server and the switch is Ok.	Reconnect the DS30 cable firmly.
		The TNs/Key0/Key1 (DNs) on the active server does not match the switch resources.	Run CW Switch Configuration Express mode to make sure the TNs/Key0/Key1 (DNs) on the active server match the switch resources	Finish CW with the right TNs/Key0/Key1, and reboot by following the procedure how to change the switch settings on CP5.0 HA NTP.
	The HA system failovers every night (around midnight).	The M1 switch has the old Controller card which would cause the temporary ÉLAN connection loss when the midnight audit was running, and the ELAN Ping failure would trigger the failover on the HA system.		Upgrade the Controller card on the switch.

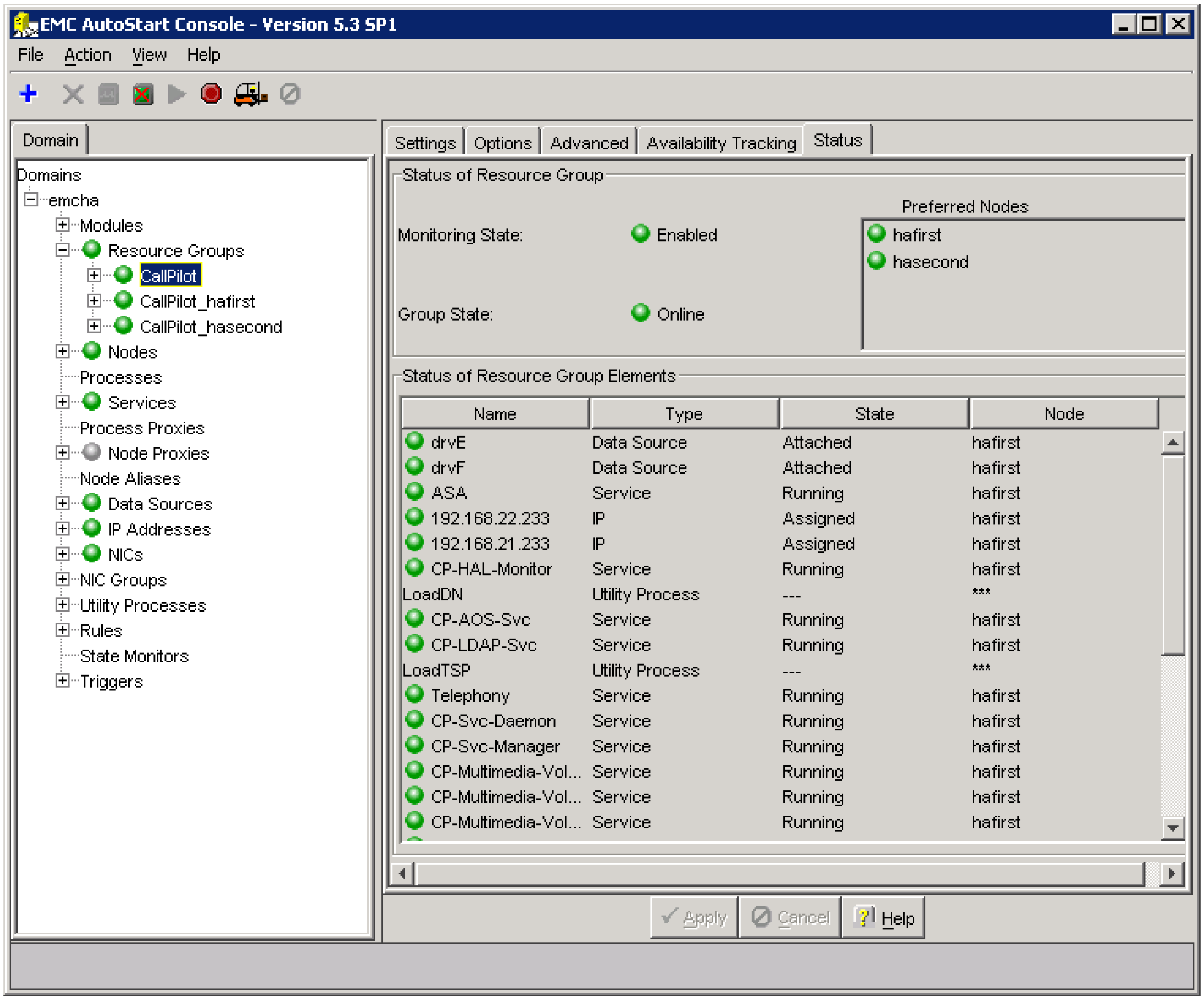
Problem Types	Symptoms	What might be wrong	Where to check	How to fix
	After the failover, the Data Sources drvE and drvF were in yellow on the AutoStart Console, and restarting AutoStart services and rebooting wouldn't help, and also manually re-synchronizing failed either.	Missing Registry keys: Please contact your Avaya support organization at this time to help troubleshoot this issue.		Please contact your Avaya support organization at this time to help troubleshoot this issue.
Importing AutoStart Definition File	Importing failed and didn't create drvE and drvF.	Forgot to add the Remote Mirror Host	The Configure Mirror Settings section on the tab Failure Detection and Mirroring of each node on AutoStart Console.	Select the right Local Mirror Address and the available Remote Mirror Host, and then click Apply, if not configured yet.
Installation	The second node failed to find the first node during the AutoStart Agent installation.	The name of the first node didn't match the real computer name of the first node.	Right click My Computer, and then click property to check the current computer name of the first node.	Make sure to enter it as the name of the first node without mistyping during the Agent installation on the second node.
	The second node failed to join the domain after installed AutoStart Agent and Console.	Didn't add the administrator account of the second node into the Valid User List of AutoStart Domain.	The Valid User List section on the License/Security tab of <Domain name> on AutoStart Console.	Add the administrator account of the second node into the Valid User List of AutoStart Domain
	Install.bat failed to find the AutoStart directory.	Entered the wrong Domain name or forgot to change the drive letter of the path or entered the wrong path of the AutoStart directory.	The AutoStart directory should be located at D:\Program Files\EMC AutoStart, and check the Domain name on the AutoStart Console.	Key in the right domain name if the previous name was wrong, or reinstalls AutoStart if the previous AutoStart directory was wrong.
		Forgot to install the AutoStart patch(es).	Search the patch's ID in D:\Program Files\EMC AutoStart\<Domain Name>\bin, D:\Program Files\EMC AutoStart\Common\bin, or D:\Program Files\EMC AutoStart\Console52\bin	Install AutoStart patches and then reboot on both nodes.
Web Applications	Reporter or other CP Web applications fail to connect to the HA system by using the Managed Host name,	The Managed Host name is not registered on the DNS server(s).	Ping the Managed Host name to see whether or not the Managed CLAN IP will be returned, if not, the Managed Host name is not registered on the DNS server(s).	Register the Managed Host name on your DNS server(s).

Problem Types	Symptoms	What might be wrong	Where to check	How to fix
	but able to connect to the HA system by using the Manage CLAN IP.			
		The wrong Managed Host name was entered when running the HA wizard	Open the AutoStart_Configuration.ini under E:\Nortel\HA to check the Managed Host name	If the wrong Managed Host name is used, you can rerun the HA wizard to correct it or simply open AutoStart_Configuration.ini under E:\Nortel\HA to change it on the active server.

Appendix E Quick troubleshooting references guide for H/A systems.

1. Normal operation of the H/A system

The normal operation of the H/A system is the situation when one of the peer Callpilot servers is online and able to process calls and another one is in standby mode. In confirmation of saying above all of the states of CallPilot in AutoStart console are green as on the following screenshot:



Status of Resource Group

Monitoring State: ● Enabled

Group State: ● Online

Preferred Nodes

● hafirst

● hasecond

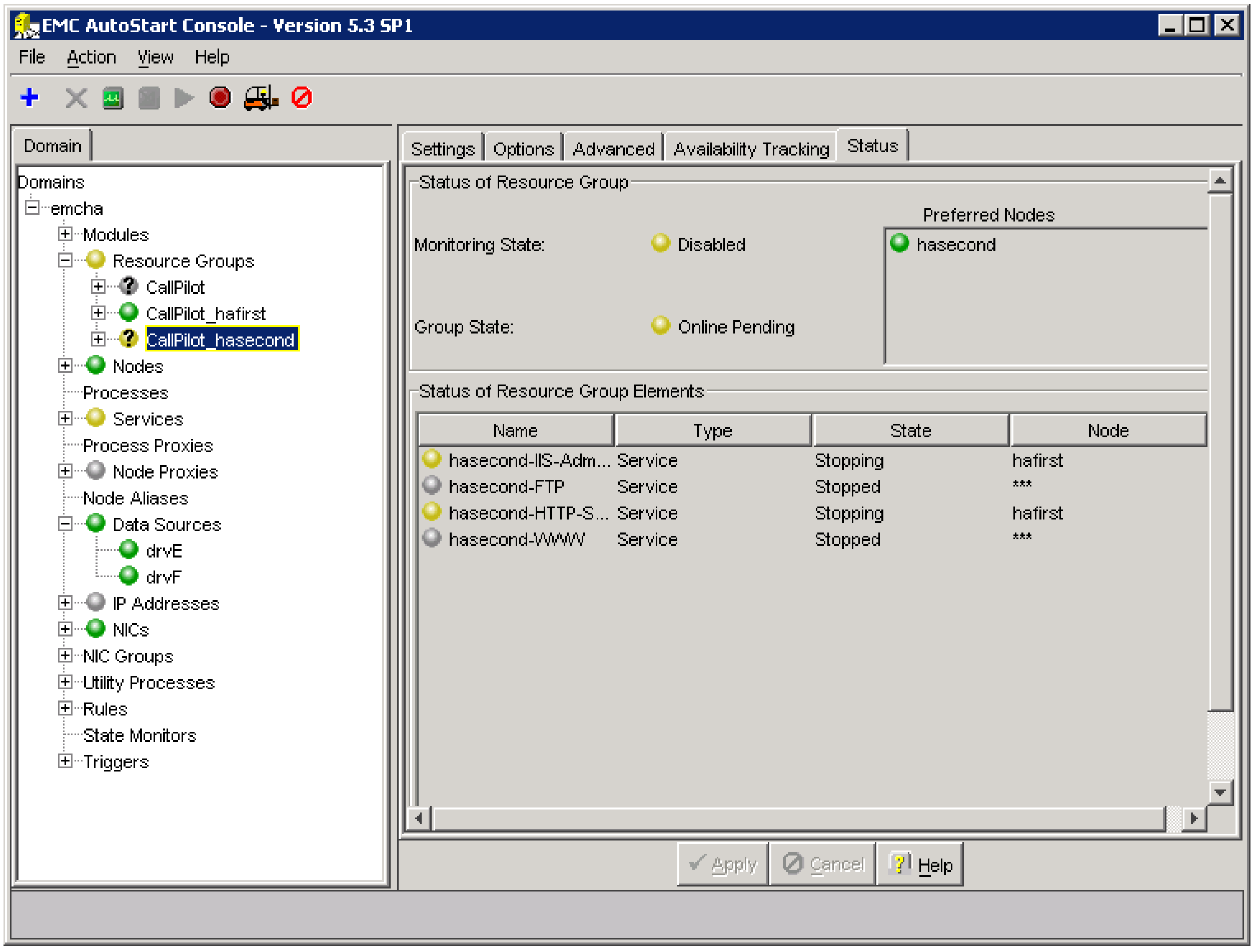
Status of Resource Group Elements

Name	Type	State	Node
● drvE	Data Source	Attached	hafirst
● drvF	Data Source	Attached	hafirst
● ASA	Service	Running	hafirst
● 192.168.22.233	IP	Assigned	hafirst
● 192.168.21.233	IP	Assigned	hafirst
● CP-HAL-Monitor	Service	Running	hafirst
LoadDN	Utility Process	---	***
● CP-AOS-Svc	Service	Running	hafirst
● CP-LDAP-Svc	Service	Running	hafirst
LoadTSP	Utility Process	---	***
● Telephony	Service	Running	hafirst
● CP-Svc-Daemon	Service	Running	hafirst
● CP-Svc-Manager	Service	Running	hafirst
● CP-Multimedia-Vol...	Service	Running	hafirst
● CP-Multimedia-Vol...	Service	Running	hafirst
● CP-Multimedia-Vol...	Service	Running	hafirst

If one of items is yellow or red, then an issue occurs on the system. See the Abnormal operation of the H/A system chapter.

2. Abnormal operation of the H/A system

This chapter refers to the situation when a failure condition is detected on the active server. In this case one of the items in the AutoStart Console could be in a yellow or red state. The following picture illustrates that several services are stopped and that cause CallPilot failure.



Status of Resource Group

Monitoring State: Disabled

Group State: Online Pending

Preferred Nodes: hasecond

Status of Resource Group Elements

Name	Type	State	Node
hasecond-IIS-Adm...	Service	Stopping	hafirst
hasecond-FTP	Service	Stopped	***
hasecond-HTTP-S...	Service	Stopping	hafirst
hasecond-WWW	Service	Stopped	***

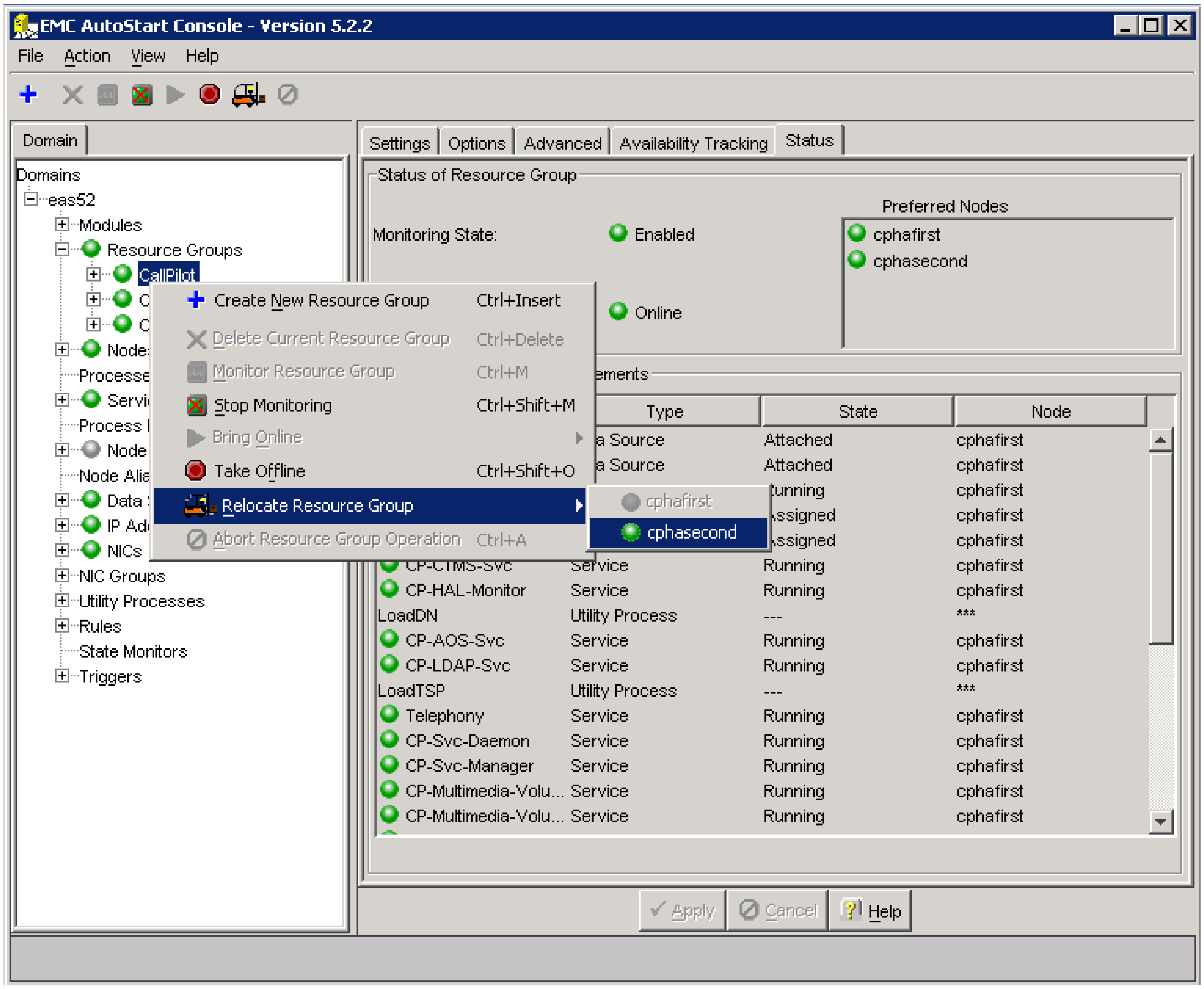
Typical cases of an Automatic Failover.
An automatic failover occurs when the AutoStart software determines that something has gone wrong on the active CallPilot server, that is, a critical CallPilot service has failed. The software initiates a failover to the standby CallPilot server without any user interaction.

Be sure that Monitoring option is enabled.

1. Some service stopped or crashed.
   CallPilot services are being monitored. AutoStart software will try to start the service 3 times in the case if service stopped. If all of the attempts are failed, then automatic failover scenario happens.
2. A reboot or shut down of the active server.
3. Optional automatic failover on the loss of connection of the ELAN at the TCP/IP level. By default, there is no failover on the Path Test failure of the Managed ELAN IP address, but it could be enabled at the setting tab of the CallPilot resource group in the Auto start console.

Manual failover.

It can be forced by administrator. To doing that, right-click Resource Groups > CallPilot, and on the shortcut menu, select Relocate Resource Group, and then select the <standby CallPilot server>.



Status of Resource Group

Monitoring State: Enabled

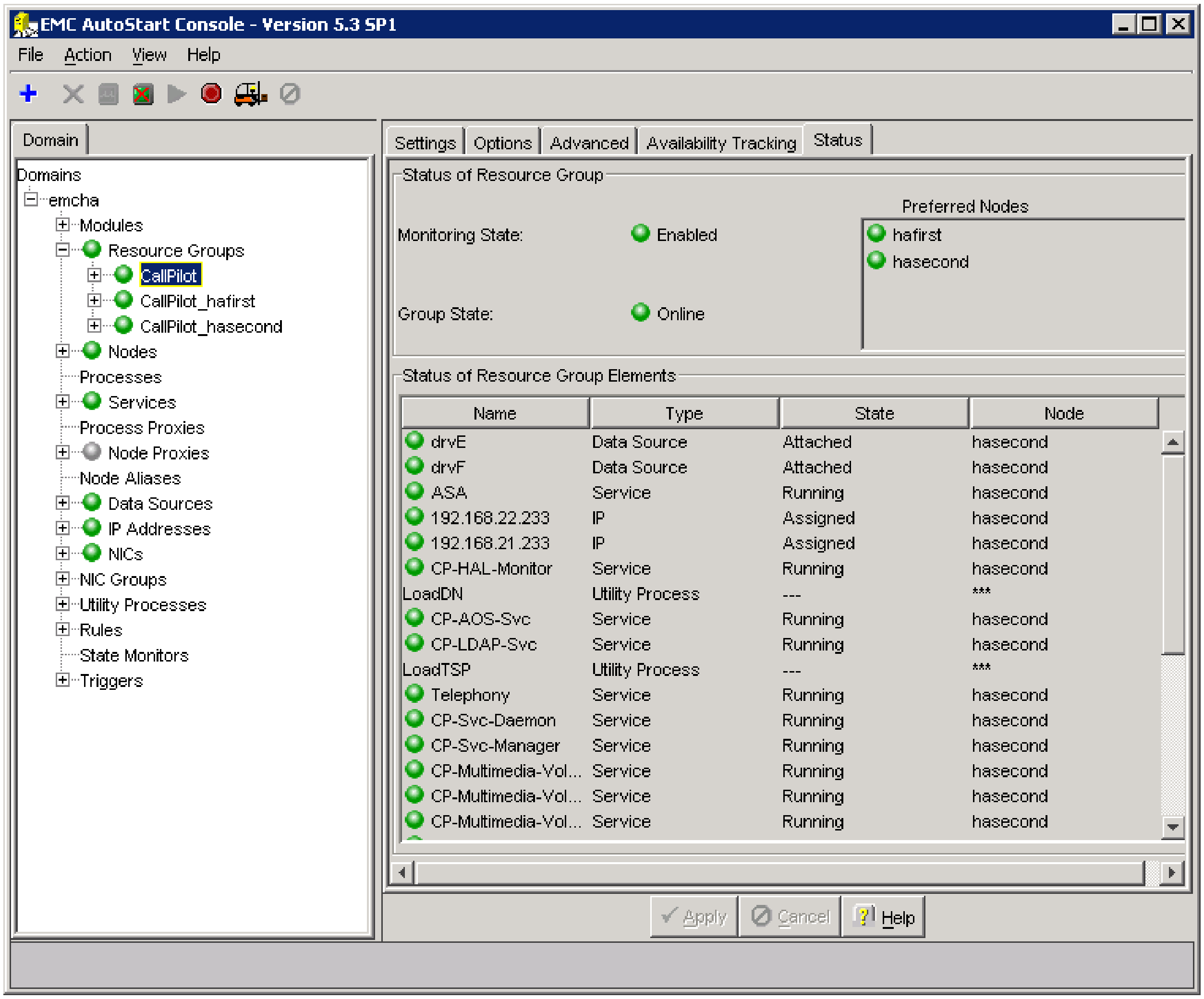
Online

Preferred Nodes:
- cphafirst
- cphasecond

	Type	State	Node
	a Source	Attached	cphafirst
	a Source	Attached	cphafirst
		unning	cphafirst
		ssigned	cphafirst
		ssigned	cphafirst
CP-CTMS-Svc	Service	Running	cphafirst
CP-HAL-Monitor	Service	Running	cphafirst
LoadDN	Utility Process	---	***
CP-AOS-Svc	Service	Running	cphafirst
CP-LDAP-Svc	Service	Running	cphafirst
LoadTSP	Utility Process	---	***
Telephony	Service	Running	cphafirst
CP-Svc-Daemon	Service	Running	cphafirst
CP-Svc-Manager	Service	Running	cphafirst
CP-Multimedia-Volu...	Service	Running	cphafirst
CP-Multimedia-Volu...	Service	Running	cphafirst

3. Successful failover

It is easy to determine if the failover passed successfully. In this case the standby server became online and the previously operational server became standby. It is shown in the AutoStart console:



Status of Resource Group

Monitoring State: Enabled

Group State: Online

Preferred Nodes
hafirst
hasecond

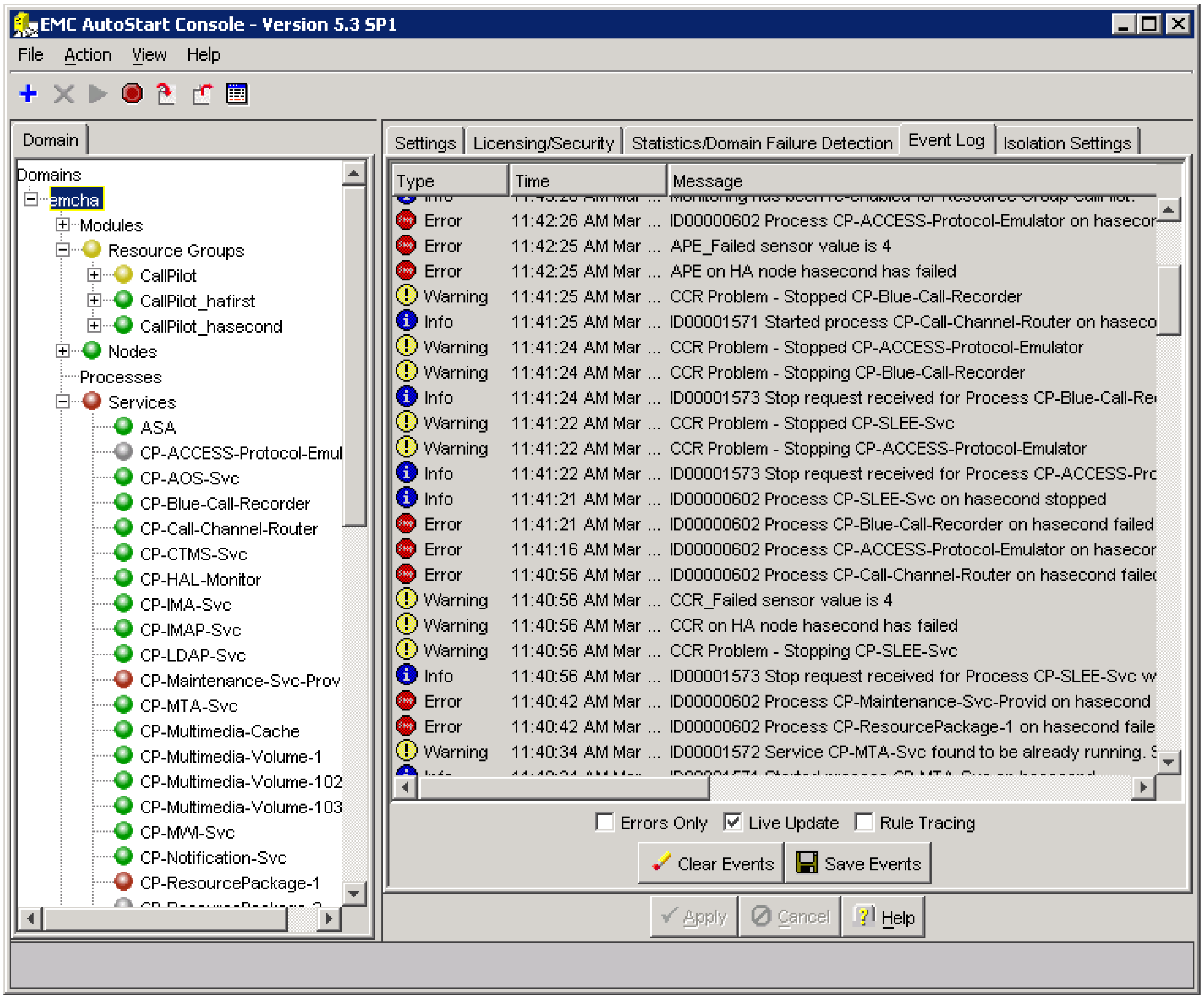
Status of Resource Group Elements

Name	Type	State	Node
drvE	Data Source	Attached	hasecond
drvF	Data Source	Attached	hasecond
ASA	Service	Running	hasecond
192.168.22.233	IP	Assigned	hasecond
192.168.21.233	IP	Assigned	hasecond
CP-HAL-Monitor	Service	Running	hasecond
LoadDN	Utility Process	---	***
CP-AOS-Svc	Service	Running	hasecond
CP-LDAP-Svc	Service	Running	hasecond
LoadTSP	Utility Process	---	***
Telephony	Service	Running	hasecond
CP-Svc-Daemon	Service	Running	hasecond
CP-Svc-Manager	Service	Running	hasecond
CP-Multimedia-Vol...	Service	Running	hasecond
CP-Multimedia-Vol...	Service	Running	hasecond
CP-Multimedia-Vol...	Service	Running	hasecond

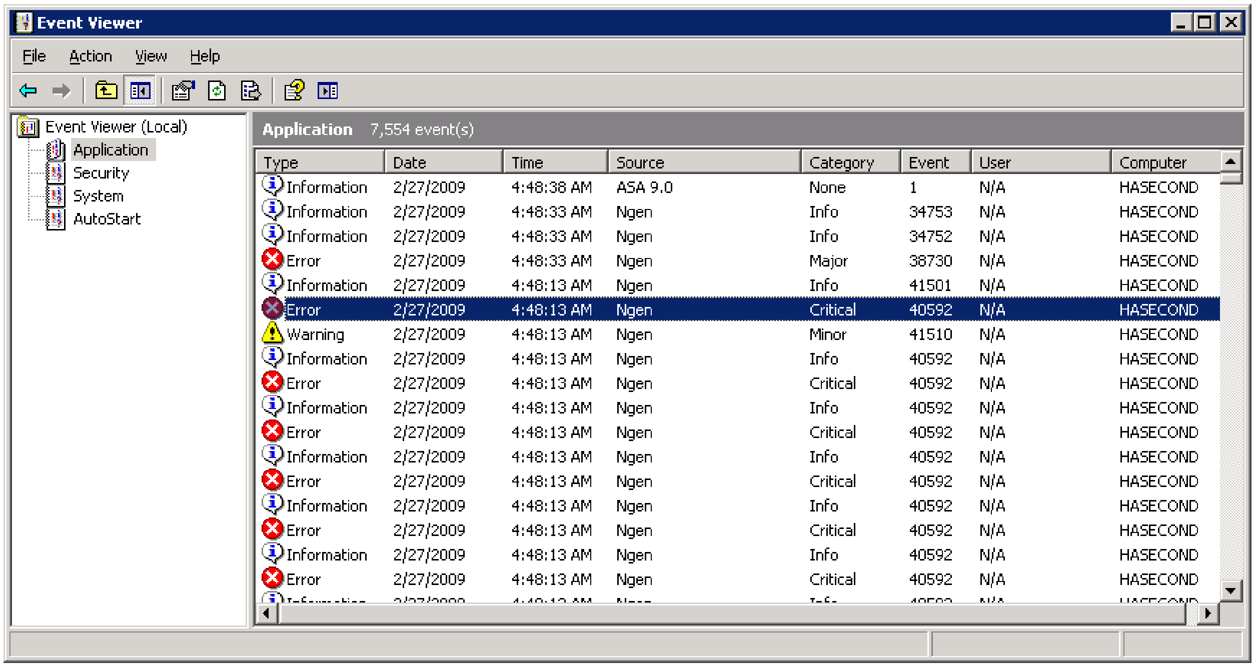
Failover operation should take up to 10-12 minutes depending on the number of resources configured and used. All the services are available for the end user as before the failover. The end user even does not know that operational server is replaced.

4. Unsuccessful failover

Failover might fail due to some reason. The most common reason of that could be a standby server that is not ready to take a failover.
If the failover fails on the standby server then an error could be found in the AutoStart console and Windows even log as on the following screenshots for example:



```
Type      Time                Message
Error     11:42:26 AM Mar ... ID00000602 Process CP-ACCESS-Protocol-Emulator on hasecor
Error     11:42:25 AM Mar ... APE_Failed sensor value is 4
Error     11:42:25 AM Mar ... APE on HA node hasecond has failed
Warning   11:41:25 AM Mar ... CCR Problem - Stopped CP-Blue-Call-Recorder
Info      11:41:25 AM Mar ... ID00001571 Started process CP-Call-Channel-Router on haseco
Warning   11:41:24 AM Mar ... CCR Problem - Stopped CP-ACCESS-Protocol-Emulator
Warning   11:41:24 AM Mar ... CCR Problem - Stopping CP-Blue-Call-Recorder
Info      11:41:24 AM Mar ... ID00001573 Stop request received for Process CP-Blue-Call-Re
Warning   11:41:22 AM Mar ... CCR Problem - Stopped CP-SLEE-Svc
Warning   11:41:22 AM Mar ... CCR Problem - Stopping CP-ACCESS-Protocol-Emulator
Info      11:41:22 AM Mar ... ID00001573 Stop request received for Process CP-ACCESS-Prc
Info      11:41:21 AM Mar ... ID00000602 Process CP-SLEE-Svc on hasecond stopped
Error     11:41:21 AM Mar ... ID00000602 Process CP-Blue-Call-Recorder on hasecond failed
Error     11:41:16 AM Mar ... ID00000602 Process CP-ACCESS-Protocol-Emulator on hasecor
Error     11:40:56 AM Mar ... ID00000602 Process CP-Call-Channel-Router on hasecond failec
Warning   11:40:56 AM Mar ... CCR_Failed sensor value is 4
Warning   11:40:56 AM Mar ... CCR on HA node hasecond has failed
Warning   11:40:56 AM Mar ... CCR Problem - Stopping CP-SLEE-Svc
Info      11:40:56 AM Mar ... ID00001573 Stop request received for Process CP-SLEE-Svc w
Error     11:40:42 AM Mar ... ID00000602 Process CP-Maintenance-Svc-Provid on hasecond
Error     11:40:42 AM Mar ... ID00000602 Process CP-ResourcePackage-1 on hasecond faile
Warning   11:40:34 AM Mar ... ID00001572 Service CP-MTA-Svc found to be already running. S
```



Application 7,554 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	2/27/2009	4:48:38 AM	ASA 9.0	None	1	N/A	HASECOND
Information	2/27/2009	4:48:33 AM	Ngen	Info	34753	N/A	HASECOND
Information	2/27/2009	4:48:33 AM	Ngen	Info	34752	N/A	HASECOND
Error	2/27/2009	4:48:33 AM	Ngen	Major	38730	N/A	HASECOND
Information	2/27/2009	4:48:13 AM	Ngen	Info	41501	N/A	HASECOND
Error	2/27/2009	4:48:13 AM	Ngen	Critical	40592	N/A	HASECOND
Warning	2/27/2009	4:48:13 AM	Ngen	Minor	41510	N/A	HASECOND
Information	2/27/2009	4:48:13 AM	Ngen	Info	40592	N/A	HASECOND
Error	2/27/2009	4:48:13 AM	Ngen	Critical	40592	N/A	HASECOND
Information	2/27/2009	4:48:13 AM	Ngen	Info	40592	N/A	HASECOND
Error	2/27/2009	4:48:13 AM	Ngen	Critical	40592	N/A	HASECOND
Information	2/27/2009	4:48:13 AM	Ngen	Info	40592	N/A	HASECOND
Error	2/27/2009	4:48:13 AM	Ngen	Critical	40592	N/A	HASECOND
Information	2/27/2009	4:48:13 AM	Ngen	Info	40592	N/A	HASECOND
Error	2/27/2009	4:48:13 AM	Ngen	Critical	40592	N/A	HASECOND
Information	2/27/2009	4:48:13 AM	Ngen	Info	40592	N/A	HASECOND
Error	2/27/2009	4:48:13 AM	Ngen	Critical	40592	N/A	HASECOND

The event 40592 shows that the CTMS Server failed to start, The CallPilot Blue Call Router service terminated and so on.

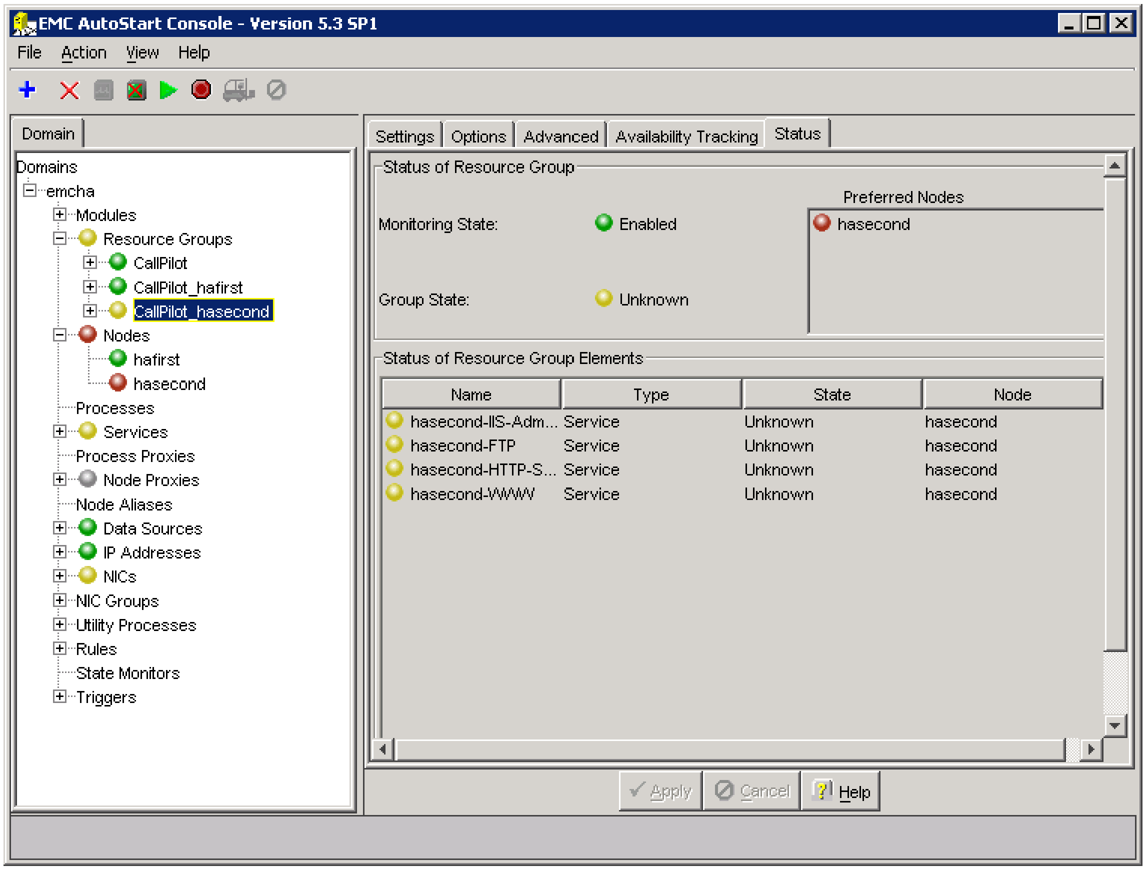
If the failover on the standby server is unsuccessful and monitoring is enabled, then the previously online server tries to start up.

5. How to be sure that the standby server is ready for a failover?

In normal operation of the HA system the standby server is ready to receive a failover. It is marked as green in the Auto start console if all the needed services for a failover are up and running.

These are the typical cases, when standby server is not ready for a failover:

1. Mandatory services are down on the standby server. Example:



Status of Resource Group

Monitoring State: Enabled

Group State: Unknown

Preferred Nodes: hasecond

Status of Resource Group Elements

Name	Type	State	Node
hasecond-IIS-Adm...	Service	Unknown	hasecond
hasecond-FTP	Service	Unknown	hasecond
hasecond-HTTP-S...	Service	Unknown	hasecond
hasecond-WWW	Service	Unknown	hasecond

<u>Solution:</u>

Manually start services marked as red or yellow.

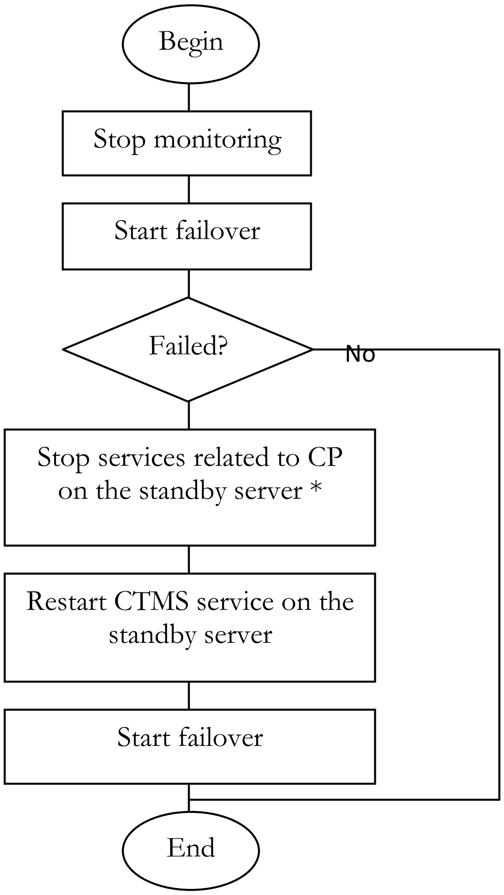
1. Special case, not visible from AutoStart console.

Sometimes standby server is in the GREEN state; however it is NOT ready to receive a failover. That could happen if there are events 36768 or 44531 in the Application Event log since the last normal operation as an online server. They are the CTMS related error events, indicating that previous CTMS session was not released properly.

<u>Solution:</u>

Manually restart the service “CTMS Server” in the Services Control panel (See diagram for details).

6. Common diagram to perform failover in case of previous failover fail


Begin
Stop monitoring
Start failover
Failed?
No
Stop services related to CP on the standby server *
Restart CTMS service on the standby server
Start failover
End

* Please stop the services, if they are started, in the following order:
CP-Time
CP-MTA
CP-IMAP
CP-IMA
CP-Notification
CP-MWI
CP-SLEE
CP-Maintenance
CP-ResourcePackage
CP-ACCESS-Protocol
CP-Blue-Call-Router
CP-Multimedia Cache
CP-Multimedia Vol 1
CP-Multimedia Vol 102
CP-Multimedia Vol 103
CP-Service-Manager

CP-Service-Daemon
Telephony
CP-LDAP
CP-AOS
CP-HAL-Monitor
ASA

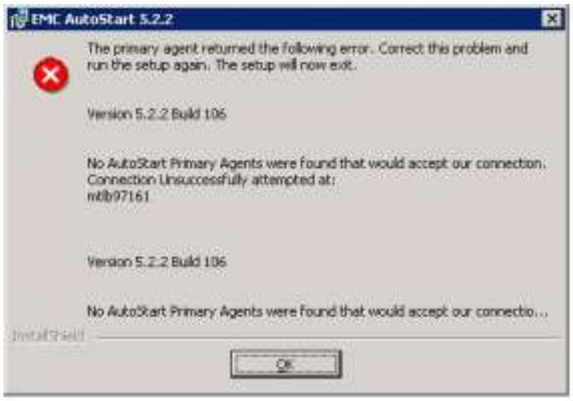
7. Other known issues and answers

1. Importing the new definition file in the AutoStart Console failed
   Solution:
   Check that all of the services are stopped and rules in the [AutoStart_Domain] > Rules are disabled. If the issue is still persists then try to delete Callpilot from the [AutoStart_Domain] > Resource Group and disks E: and F: from the [AutoStart_Domain] > Data Sources.
2. Some services couldn’t be started while the Callpilot Bringing online
   Solution:
   Check the account settings in the [AutoStart_Domain] > Utility Process for the following services: DisableAOS, KillServices, LoadDN, LoadTSP, UnloadTSP, UnloadTSPOnStandbyServer.

Please refer to the NTP NN44200-311 for any H/A specific information and NTP NN44200-700 for common troubleshoot.

8. EMC AutoStart installation error

When configuring EMC AutoStart software on CP2, the following pop-up window may appear if the EMC AutoStart Transport Service is disabled:



The primary agent returned the following error. Correct this problem and run the setup again. The setup will now exit.

Version 5.2.2 Build 106

No AutoStart Primary Agents were found that would accept our connection.
Connection Unsuccessfully attempted at:
mtlb97161

Version 5.2.2 Build 106

No AutoStart Primary Agents were found that would accept our connectio...

Workaround: Ensure the EMC AutoStart Transport Service is enabled and re-attempt the installation and configuration.

Appendix F CallPilot High Availability and Contact Center Integration

CallPilot 5.1 High Availability (H/A) integration with Contact Center CCMS 6.0 or 7.0 involves three primary scenarios:

- Implementing a complete new H/A and CCMS integration
- Adding CCMS integration on an existing H/A system
- Upgrading an existing CP/CCMS integration to H/A

These scenarios involve updates to the switch, Contact Center, and CallPilot, involving a number of different steps and several different documents. The intent of the following is to provide a high-level "task list" to ensure installation success and also provide details on troubleshooting and verification of a successful deployment.

Documentation reference:
The following documentation should be readily available when implementing any of the scenarios noted above:

Document	Description
NTP NN44200-311	CallPilot High Availability Installation and Configuration Guide
NN49000-310	Solution Integration Guide for Communication Server 1000, CallPilot, and Contact Center
NTP 297-2183-931	Contact Center CS1000/M1 and CallPilot Voice Processing Guide
DTR-2005-0392-Global	Contact Center 6 Distributor Technical Reference (DTR) rev-25 or later
	CC6.0 Support for CallPilot High Availability Tech Transfer Slides
CallPilot 5.1 - Distributor Technical Reference	This document
SU/PEP readme files	Supplemental instructions within each SU/PEP for the products.
	CallPilot High Availability Training Video
	Course #6350W / CallPilot High Availability (with supplemental Contact Center Integration)

Scenario-based Task Lists

<u>Scenario A. (Implementing a new CallPilot HA and CCMS integration solution.)</u>

1. Install all components as per product NTPs (CallPilot and Contact Center) and associated DTRs.

For CallPilot specifically, reference NTP NN44200-311 / CallPilot High Availability Installation and Configuration Guide to configure new CallPilot H/A system.

<u>Scenario B. (Adding CCMS integration to an existing CallPilot HA system.)</u>

Below are the required steps;

1. Verify PBX Patches & resources needed in CS1000 (Configure PBX per Solution Integration NTP NN49000-300). Ensure the following PBX updates are installed:
   a. Communication Server 1000 (CS 1000) Release 5.0
      i. PEP MPLR24673

    b. Communication Server 1000 (CS 1000) Release 5.5
        i. PEP MPLR24673
        ii. PEP MPLR26727 (only if Signaling Server is present)
    c. Communication Server 1000 (CS 1000) Release 6.0
        i. MPLR23630 (merges MPLR24673 and MPLR26727)
        ii. MPLR30461
    d. Communication Server 1000 (CS 1000) Release 7.0
        i. MPLR30461
2. Configure PBX per Solution Integration NTP NN49000-310
    a. Configure the separate ELAN for the CC
    b. Configure system parameters (NCR, CSQI, CSQO)
    c. Configure the ACD services (ADS block)
    d. Create the ACD-DN for Contact Center / IVR ports
    e. Create the ACD-DN for Contact Center / ACCESS ports
    f. Create voice ports (agent TNs) for IVR ACD queue
        i. **Note**: Half of the ports must be created using the TNs from the "Active" CallPilot MGate card(s) and the other half from the standby CallPilot MGate card(s).
    g. Create voice ports (agent TNs) for the ACCESS ACD queue
        i. **Note:** Half of the ports must be created using the TNs from the "Active" CallPilot MGate card(s) and the other half from the standby CallPilot MGate card(s).
    h. Configure at least one CDN for Contact Center
3. Upgrade the CallPilot to CP50041SU06S and CP500S06G08C, strictly adhering to steps in the readme. This needs to occur on both the active and standby servers.
4. Run the Configuration Wizard on both CallPilot servers to allocate channels for Contact Center ACCESS and IVR ports as described in NTP NN49000-310. On the switch information page:
    a. Check the "Enable Symposium Call Center Server Integration" option
    b. Enter the Call Center server IP address
    c. Configure IVR channels for the Call Center which you have configured in the PBX
    d. Configure ACCESS channels for the Call Center which you have configured in the PBX.
        i. **Note**: All ACCESS channels must have unique (for both notes) numbers in the "Class ID" column
    e. Add the ACCESS and IVR ACD-DNs to the SDN table. Application Name must be "Symposium Voice Service".
5. Verify Contact Center Patches are up to date.
    a. Contact Center (CCMS) 6.0:
        i. Service Update CCMS_6.0_SU08;
        ii. Service Update Supplementary: CCMS_6.0_SUS_0801 and CCMS_6.0_SUS_0802 and CCMS_6.0_SUS_0803
        iii. PEP CCMS_6.0_DP_060313 (Requires CC GPS support to download to server)
    b. Contact Center (CCMS) 7.0:
        i. Service Update CCMS_7.0_SU_0301 and CCMS_7.0_SU_0302 and CCMS_7.0_SU_0303 and CCMS_7.0_SU_0304
6. Run the CCMS Server Setup Config as described IN NTP NN49000-310 (don't reboot)
    a. On the Voice Services page set:
        i. Voice Connection Type to "TCP" (CallPilot)
        ii. CallPilot HA to "YES"
    b. On the Voice Service page enter:
        i. Managed ELAN IP as CallPilot Server IP
        ii. Managed CLAN IP

7. Configure CCMA resources to Solution Integration NTP NN49000-310
    a. Acquire the CDN which you have created in the PBX
    b. Acquire the IVR and ACCESS ACD-DNs which you have created on the PBX
    c. Configure the Contact Center Global Settings
        i. Note: Default ACCES IVR DN should be set to the ACCESS ACD queue.
    d. Acquire ACD agent voice ports which you have created on the PBX
        i. Note: Only those ports which belong to active CallPilot should change status to "Acquired login"
        ii. Note: Only ACCESS ports should have anything in the "Channel" column and it must be "Class ID" of this channel which you have entered in CallPilot Config Wizard
8. Reboot CCMS
9. Take the CallPilot resource group offline
10. Reboot both CallPilot servers
11. Bring Resource group on line once CCMS is fully operational.

Scenario C (Existing CallPilot 1005r with contact center integration)

Below are the required steps;

1. Verify required PBX updates are installed:
    a. Communication Server 1000 (CS 1000) Release 5.0
        i. PEP MPLR24673
    b. Communication Server 1000 (CS 1000) Release 5.5
        ii. PEP MPLR24673
        iii. PEP MPLR26727 (only if the Signaling Server is present)
    c. Communication Server 1000 (CS 1000) Release 6.0
        i. MPLR23630 (merges MPLR24673 and MPLR26727)
        ii. MPLR30461
    d. Communication Server 1000 (CS 1000) Release 7.0
        i. MPLR30461
2. Configure PBX resources for the second node per NTP NN44200-312.
3. Configure the second CP voice ports on the PBX for CC per NTP NN49000-310
    Note: Number of the IVR voice ports on the second CP must be equal to the number of these ports on the first CP.
4. **Note:** Number of the Access voice ports on the second CP must be equal to the number of these ports on the first CP.
5. Upgrade the CallPilot to CP50041SU06S & CP500S06G08C strictly adhering to steps in the readme. This needs to occur on both the active and standby servers.
6. Run the Configuration Wizard on both CP nodes.
7. Follow the Feature Expansion using the High Availability: Installation and Configuration Guide NN44200-311
    a. Note: CCMS integration is not mentioned in this guide.
    b. When running Configuration Wizard make sure to define CCMS IP address and Ports.
    c. Do not bring resource group on-line at this time

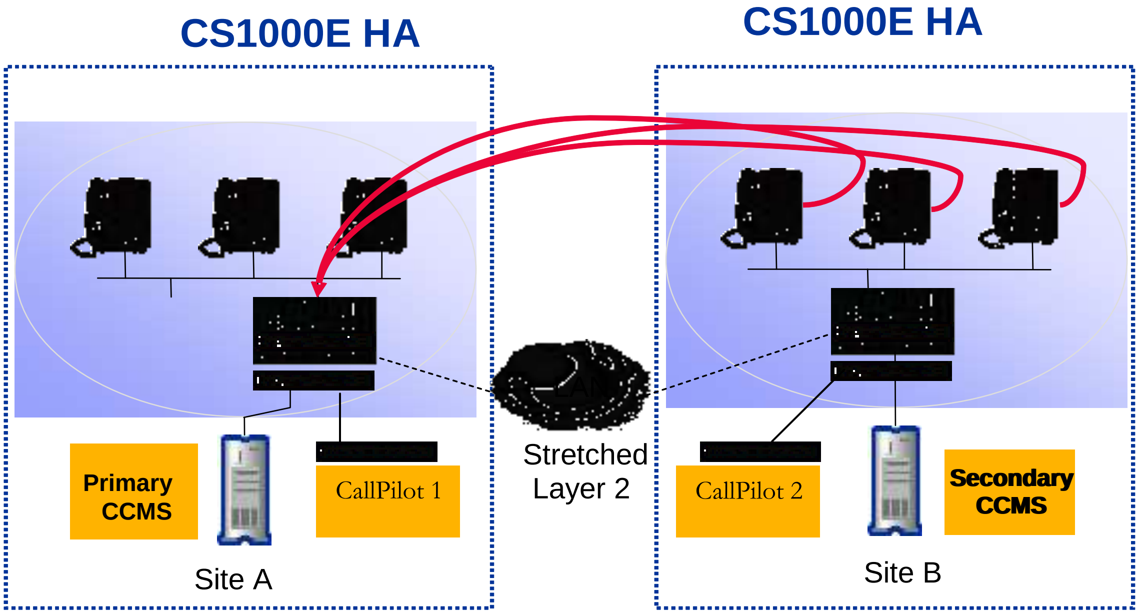
8. Run Configuration Wizard on the new CP node to allocate channels for the CC Access and IVR ports as described in NTP NN49000-310. On the switch information page:
   a. Check the "Enable Symposium Call Center Server Integration" option
   b. Enter the Call Center IP
   c. Configure IVR channels for the Call Center which you have configured on the PBX
   d. Configure Access channels for the Call Center which you have configured on the PBX
   Note: All Access Channels must have unique (for both nodes) number in the "Class ID" column
9. Verify Contact Center Patches are up to date.
   a. Service Update CCMS_6.0_SU_08;
   b. Service Update Supplementary: CCMS_6.0_SUS_0801 and CCMS_6.0_SUS_0602 and CCMS_6.0_SUS_0603
   c. PEP CCMS_6.0_DP_060313 (Requires CC GPS support to download to server)
   d. CCMS, CCMA.
10. Run the CCMS Server Setup Config as described in NTP NN49000-310
    a. On the Voice Services page set:
       Voice Connection Type to TCP (CallPilot)
       CallPilot HA to "Yes"
    b. On the Voice Services page enter:
       Managed ELAN IP as CallPilot Server IP
       Managed CLAN IP
11. Configure CCMA resources according to Solution Integration NTP NN49000-310:
    a. Acquire the CDN which you have created on the PBX
    b. Acquire the IVR and Access ACDs which you have created on the PBX
    c. Configure the CC global settings.
       i. Note: Default Access IVR DN should be set to the ACCESS ACD queue
    d. Acquire ACD agent voice ports which you have created on the PBX
       i. Note: Only those ports which belongs to active CP should change their status to "Acquired login"
       ii. Note: Only Access ports should have anything in the "Channel" column and it must be "Class ID" of this Channel which you have entered earlier in CP Config Wizard
12. Reboot CCMS
13. Take the CallPilot resource group offline
14. Reboot both CallPilot servers
15. Bring the CallPilot resource group on-line.

Appendix G CCMS Geo-Campus with CallPilot stand-alone and GR configurations

NOTE: For CallPilot systems integrated with Contact Center for voice services, the recommended solution is High Availability. H/A provides an automatic failover offering with minimal service disruption to Contact Center voice services. Unfortunately, H/A requires both servers be co-located and implemented at one site, making it unsuitable in a Geo-Campus configuration. As such, CallPilot Geographic redundancy can be used as an alternative, but will require manual intervention if a failover should ever occur. This administration activity can be accomplished a number of different way, each with their advantages and disadvantages depending on overall system size/configuration. Below outlines one possible option using GR.

This document covers the following:
1. CCMS GeoCampus with standalone CallPilot at each Site
2. CCMS GeoCampus with Geo Redundant CallPilot and replicated Mailboxes

Configuration #1
CCMS Geo-Campus with standalone CallPilot at each Site



Each CallPilot connects to the CCMS managed CLAN IP with Telephony disabled on the CallPilot connected to standby CCMS.

CCMS will only connect to the CallPilot at the local site.

Installation and Commissioning

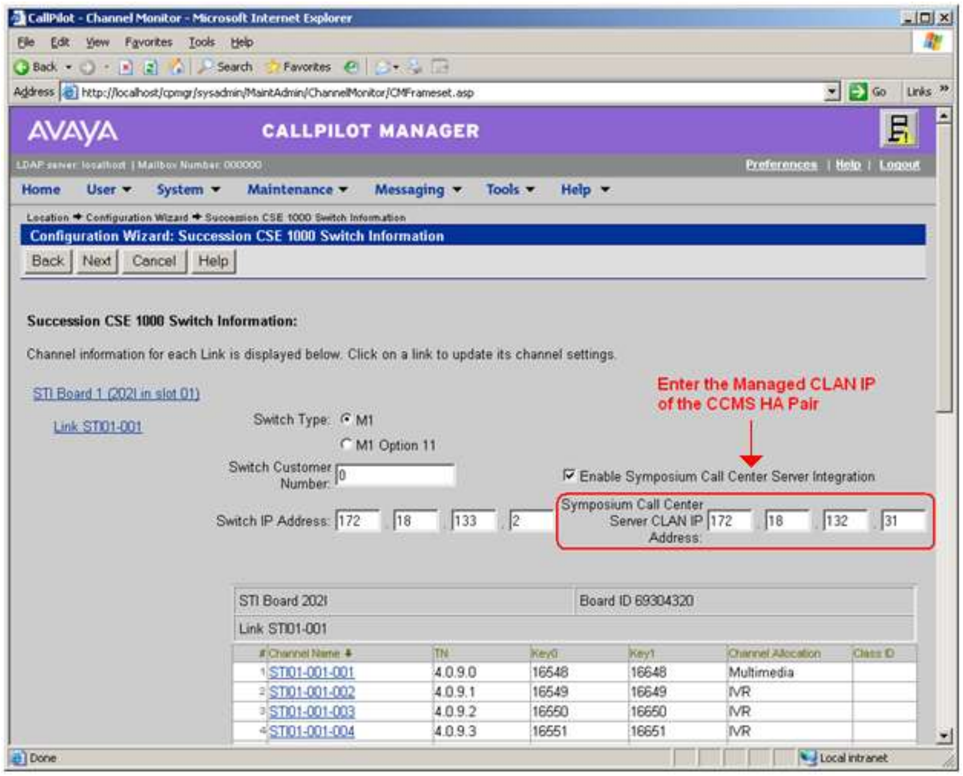
For installation of AACC Application Redundancy please refer this paper assumes from this point that R&R has been commissioned as per the Avaya Aura™ Contact Center Commissioning Guide (NN44400-312), Configuring "High Availability Campus co-resident server Commissioning"

In this configuration, when installing and configuring the CallPilot systems, the CallPilot access ports should be configured with different ACD DN's per site. The Channel ID's for the Access ports should be unique between the 2 sites and each CallPilot will need to declare different Access DN's in the SDN table. In the event of a switchover, the scripts will not need to be modified to change the provisioning for IVR and Control Voice Session call treatment. To allow for a smooth transition to the Standby Site, the Script variables should be used in the Contact Center Scripting when referring to the IVR and Access ports.

(i) OPEN VOICE SESSION….. PLAY PROMPT <variable>
(ii) GIVE IVR < variable>

Switch Configuration as setup in CallPilot Manager

When configuring CallPilot to work with CCMS the managed CLAN should be entered in the switch settings page of the CallPilot configuration wizard. Enter the unique TN details for the local CallPilot. Remember to keep the Access Port Channel IDs unique on both CallPilots.


CallPilot - Channel Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/cpmgr/sysadmin/MaintAdmin/ChannelMonitor/CMFrameset.asp
Go Links
AVAYA
CALLPILOT MANAGER
LDAP server: localhost | Mailbox Number: 000000
Preferences | Help | Logout
Home User System Maintenance Messaging Tools Help
Location → Configuration Wizard → Succession CSE 1000 Switch Information
Configuration Wizard: Succession CSE 1000 Switch Information
Back Next Cancel Help
Done
Local intranet

Succession CSE 1000 Switch Information:

Channel information for each Link is displayed below. Click on a link to update its channel settings.

STI Board 1 (202I in slot 01)
Link STI01-001

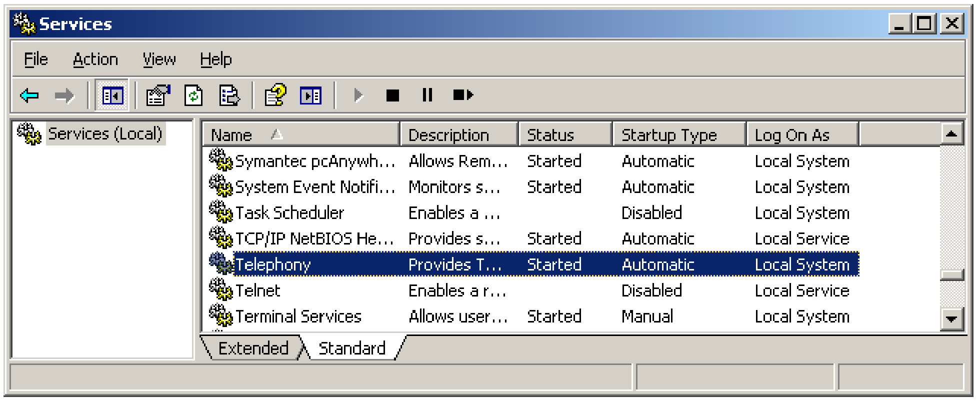
Enter the Managed CLAN IP of the CCMS HA Pair

Switch Type: ● M1 ○ M1 Option 11
Switch Customer Number: 0
☑ Enable Symposium Call Center Server Integration
Switch IP Address: 172 . 18 . 133 . 2
Symposium Call Center Server CLAN IP Address: 172 . 18 . 132 . 31

STI Board 202I | Board ID 69304320
Link STI01-001

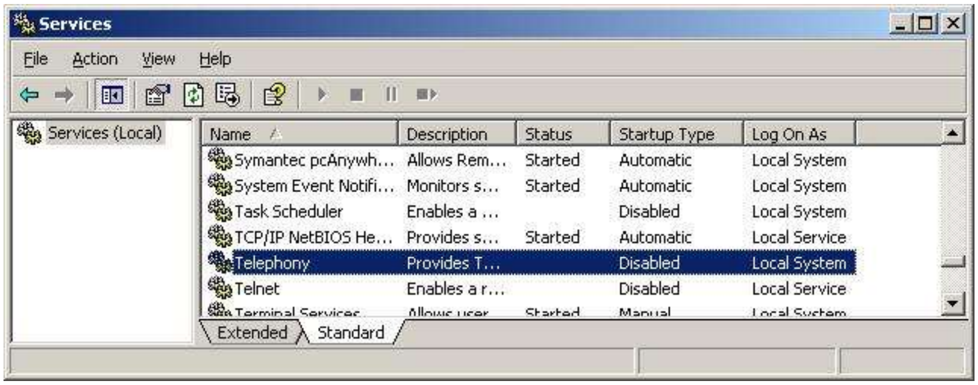
#	Channel Name	TN	Key0	Key1	Channel Allocation	Class ID
1	STI01-001-001	4.0.9.0	16548	16648	Multimedia	
2	STI01-001-002	4.0.9.1	16549	16649	IVR	
3	STI01-001-003	4.0.9.2	16550	16650	IVR	
4	STI01-001-004	4.0.9.3	16551	16651	IVR	

Under the windows services on the CallPilot at the active Site A, the Telephony Service should be at its default value of Automatic and running.



Name	Description	Status	Startup Type	Log On As
Symantec pcAnywh...	Allows Rem...	Started	Automatic	Local System
System Event Notifi...	Monitors s...	Started	Automatic	Local System
Task Scheduler	Enables a ...		Disabled	Local System
TCP/IP NetBIOS He...	Provides s...	Started	Automatic	Local Service
Telephony	Provides T...	Started	Automatic	Local System
Telnet	Enables a r...		Disabled	Local Service
Terminal Services	Allows user...	Started	Manual	Local System

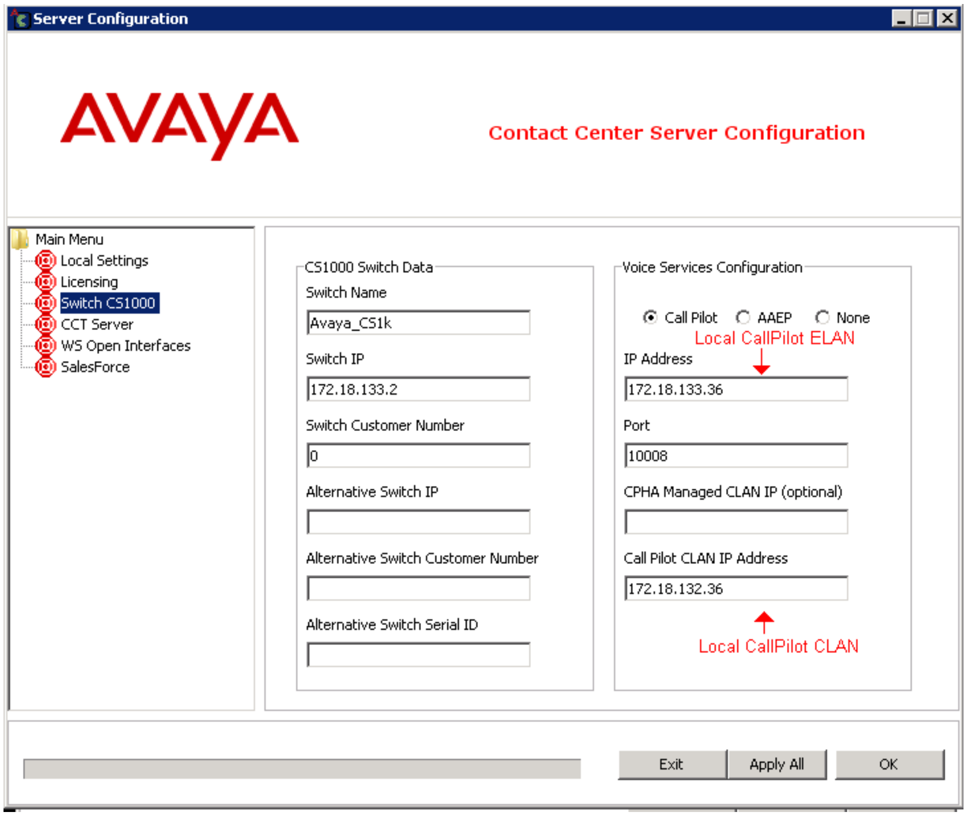
On the CallPilot at the standby Site B, under the windows services stop the Telephony Service and set it to "Disabled"



Name	Description	Status	Startup Type	Log On As
Symantec pcAnywh...	Allows Rem...	Started	Automatic	Local System
System Event Notifi...	Monitors s...	Started	Automatic	Local System
Task Scheduler	Enables a ...		Disabled	Local System
TCP/IP NetBIOS He...	Provides s...	Started	Automatic	Local Service
Telephony	Provides T...		Disabled	Local System
Telnet	Enables a r...		Disabled	Local Service
Terminal Services	Allows user	Started	Manual	Local System

In the event of a CCMS switchover:
Manual intervention is required to bring the 2nd CallPilot into service. On the original active (primary) CallPilot set the Telephony service will be stopped and the service set to disabled as detailed above. Then set the telephony service to Automatic and running on the original standby (secondary) CallPilot and restart the server.

On the CCMS server launch the Server Configuration Utility. Select the CallPilot radio button and enter the ELAN, Port Number and CLAN of the local CallPilot.



CS1000 Switch Data

Switch Name: Avaya_CS1k

Switch IP: 172.18.133.2

Switch Customer Number: 0

Alternative Switch IP:

Alternative Switch Customer Number:

Alternative Switch Serial ID:

Voice Services Configuration

● Call Pilot ○ AAEP ○ None

IP Address: 172.18.133.36

Port: 10008

CPHA Managed CLAN IP (optional):

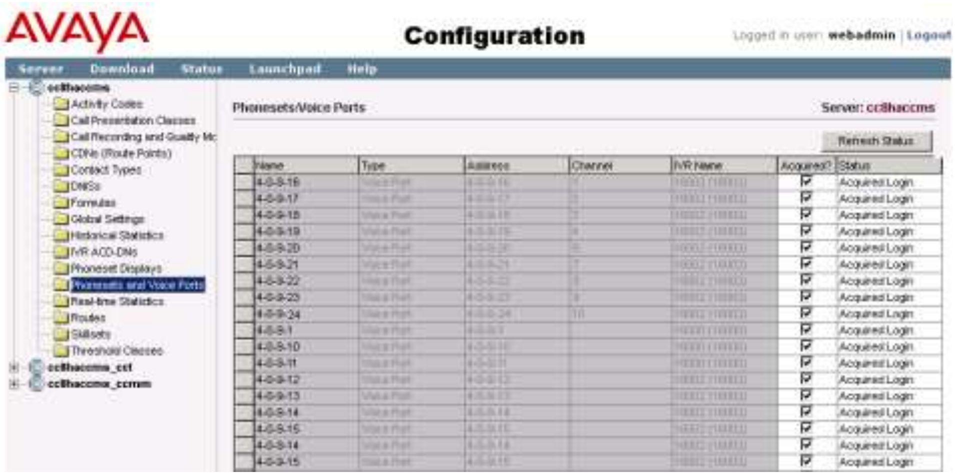
Call Pilot CLAN IP Address: 172.18.132.36

Local CallPilot ELAN

Local CallPilot CLAN

In CCMA / Configuration / Phonesets and Voice Ports add all Voice Ports from both CallPilots.

Make sure only the local CallPilot ports are acquired and logged in, the standby CallPilot ports should not be acquired – this is a manual step.

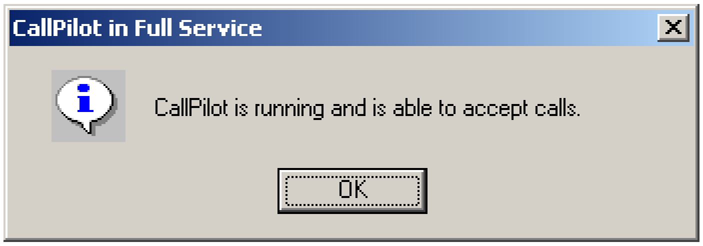


Phonesets/Voice Ports

Server: cc8haccms

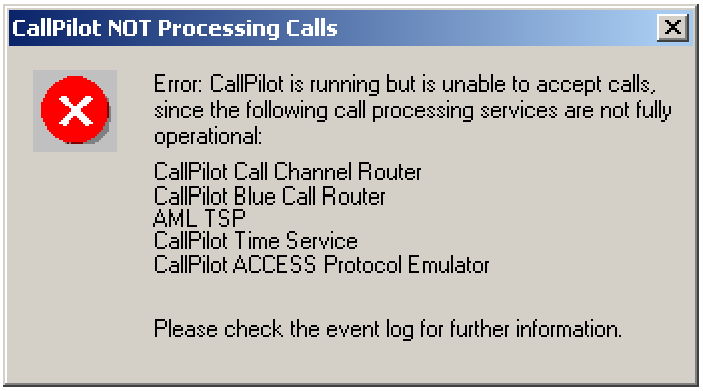
Name	Type	Address	Channel	IVR Name	Acquired?	Status
4-0-9-16	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-17	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-18	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-19	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-20	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-21	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-22	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-23	Voice Port	[illegible]	[illegible]	[illegible]	☑	Acquired Login
4-0-9-24	Voice Port	[illegible]	10	[illegible]	☑	Acquired Login
4-0-9-1	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-10	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-11	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-12	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-13	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-14	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-15	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-14	Voice Port	[illegible]		[illegible]	☑	Acquired Login
4-0-9-15	Voice Port	[illegible]		[illegible]	☑	Acquired Login

When the systems are up and running the CallPilot on the active site will be running and able to accept calls:



CallPilot is running and is able to accept calls.

The CallPilot on site B which has the Telephony Service Disabled will show booting for up to 30 minutes and finally return the message "CallPilot NOT Processing Calls".



Error: CallPilot is running but is unable to accept calls, since the following call processing services are not fully operational:

CallPilot Call Channel Router
CallPilot Blue Call Router
AML TSP
CallPilot Time Service
CallPilot ACCESS Protocol Emulator

Please check the event log for further information.

Resiliency Deployment Considerations

The CallPilots will have to be backed up regularly and restored to make sure the CallPilot Prompts and applications are kept up to date.

In the Server Configuration on CCMS, the CallPilot on the Primary will have a different IP address than the CallPilot on the Secondary as they are two separate systems. If changes are made on the Active CCMS Server Configuration, then the Standby CCMS will also have to be updated at the same time.

Always check that the Switch IP and CallPilot information is correct for each CCMS before automatic switchovers are enabled, or a manual switchover is performed.

Resiliency Deployment Examples

Example Site Configuration

Site A
Call Server at Site A is the Primary Call Server.
CCMS at Site A is the normally Primary CCMS.
CallPilot 1 is the normally Active CallPilot Server; it has IVR and ACCESS Ports.
Contact Center Agents are configured at Site A.
CCMS A is configured to point to CS Primary and CallPilot 1.
CallPilot 1 is configured to point to CS Primary and CCMS A.

Site B
Call Server at Site B with the CS1K split Core.
CCMS at Site B is the normally Standby with Replication from Site A.
CallPilot 2 is the normally Inactive CallPilot Server, it has IVR and ACCESS Ports.
Contact Center Agents are configured at Site B.
CCMS B is configured to point to CS1K and CallPilot 2.
CallPilot 2 is configured to point to CS1K and CCMS B.

Under normal operation Call Server at Site A is Active along with CCMS A and CallPilot 1 at Site A.

CCMS Access Ports Configuration
CallPilot 1 TNs (IVR, Access ports) are acquired.
Call Server at Site B is Inactive and CCMS B is on Standby.
CallPilot 2 TNs (IVR, Access ports) are created and visible from CCMA when connected to CCMS A. All these are replicated to CCMS B, they are NOT acquired and logged in as CallPilot 2 is not in service, the IVR ports will appear as "Acquired Logout" and the Access ports will show "Acquire Failed".

Scripting Requirements

Scripting provisioned for IVR and Control Voice Session call treatment.

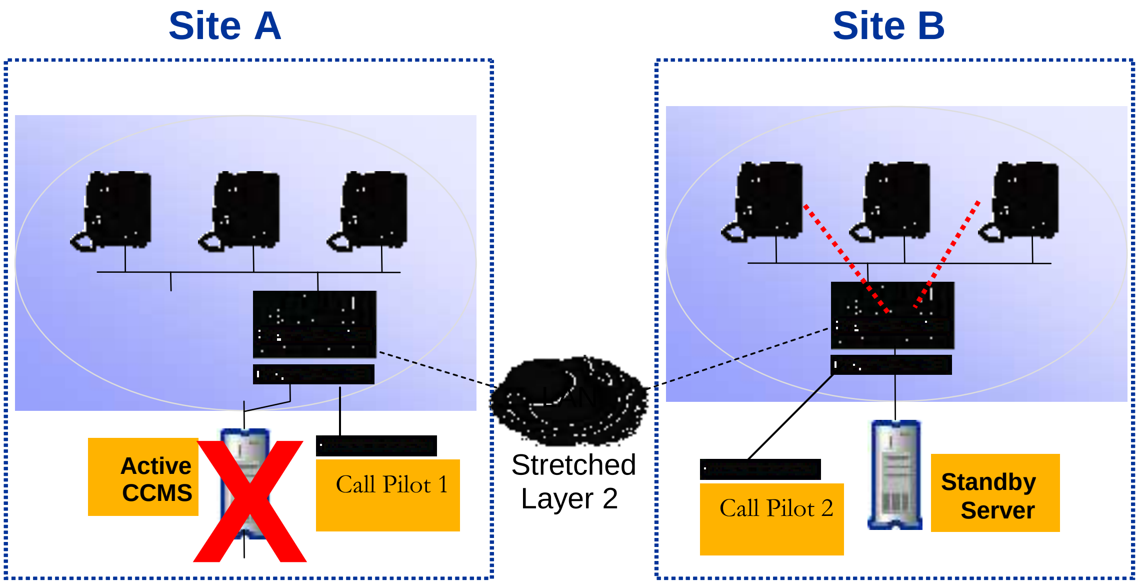
To allow for a smooth transition to the Standby Site, the Script variables should be used in the Contact Center Scripting when referring to the IVR and Access ports.

(i) OPEN VOICE SESSION….. PLAY PROMPT <variable>
(ii) GIVE IVR < variable>

This means that on a switchover, the Script variables can be modified to utilise the IVR and the Access ports on the Standby Site

Manual IVR calls and Access calls are successful but only the CallPilot ports at Site A service calls.

Switchover Scenario #1: CCMS Failover

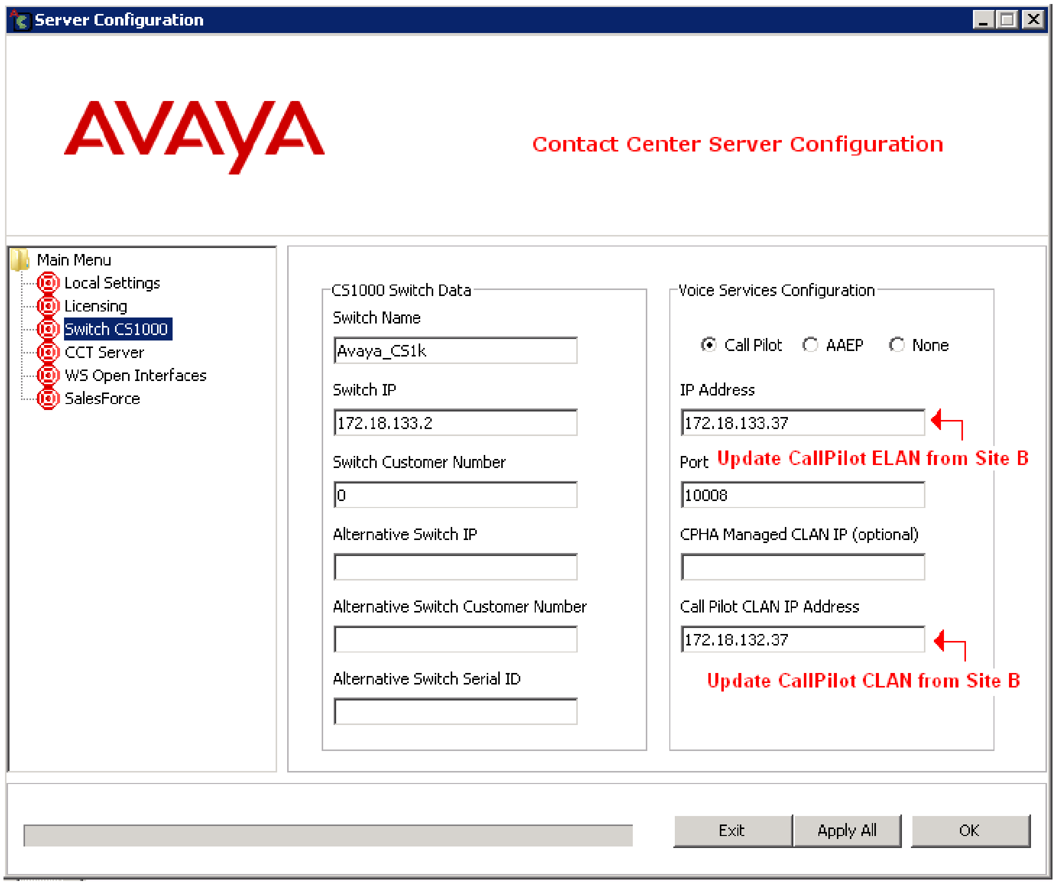


In the event of a CCMS failure, the Standby CCMS will come online. The Standby CCMS Server Setup Configuration needs to be checked to make sure that the Standby site is connected to the correct CallPilot. If the incorrect CallPilot is in use, then the configuration settings for the CallPilot need to be changed on the Standby server and the CCMS restarted.

For changing the Switch Information, follow the steps in “Avaya Contact Center Server Administration Guide” and section “Contact Center Manager Server - Changing the Communication Server 1000 switch data”

Manual intervention is required at this point for CCMS B:

- Disable the Telephony Service and stop it on CallPilot at Site A
- Enable the Telephony Service and start it on CallPilot at Site B
- In Server Configuration point to the CallPilot at Site B:
- De-acquire Site A IVR ports
- De-acquire Site A ACCESS ports
- Acquire Site B IVR ports
- Acquire Site B ACCESS ports
- Modify script accordingly the allow calls to get Voice treatment on Site B.



Contact Center Server Configuration

CS1000 Switch Data

Switch Name: Avaya_CS1k

Switch IP: 172.18.133.2

Switch Customer Number: 0

Alternative Switch IP:

Alternative Switch Customer Number:

Alternative Switch Serial ID:

Voice Services Configuration

● Call Pilot ○ AAEP ○ None

IP Address: 172.18.133.37

Update CallPilot ELAN from Site B

Port: 10008

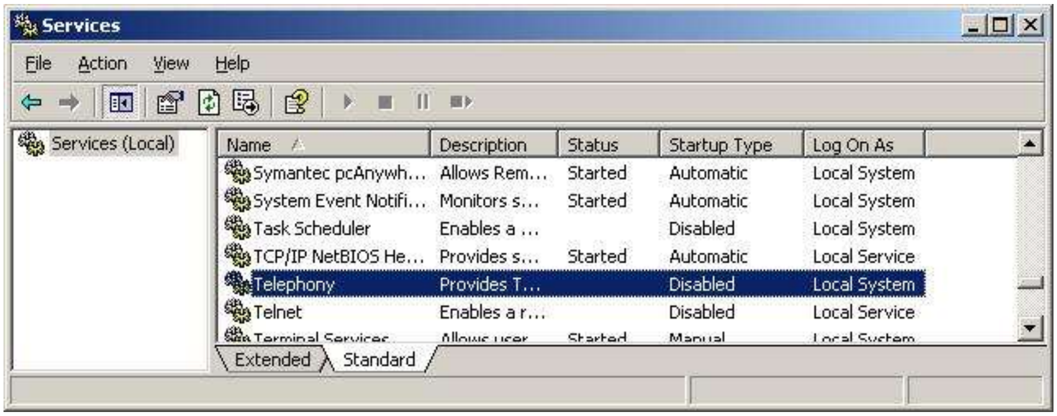
CPHA Managed CLAN IP (optional):

Call Pilot CLAN IP Address: 172.18.132.37

Update CallPilot CLAN from Site B

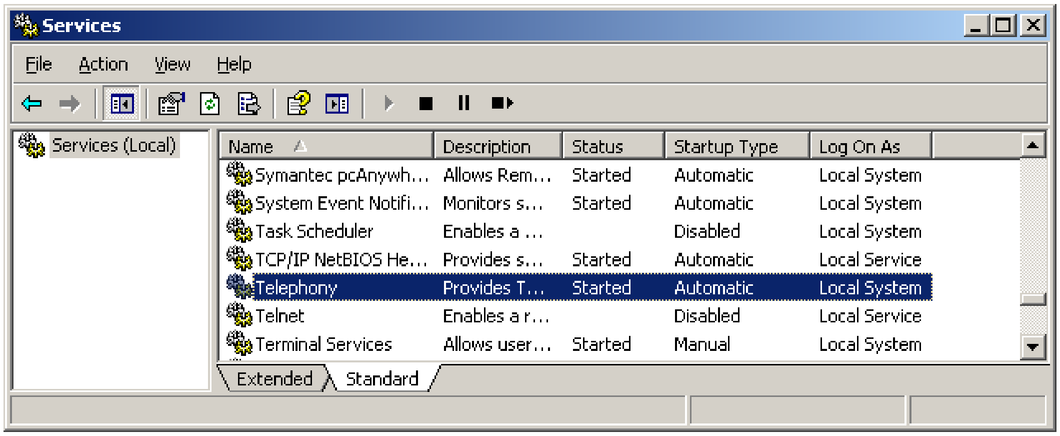
On the CallPilot at Site A, under the windows services stop the Telephony Service and set it to “Disabled”.

This will also stop the “Remote Access Connection Manager” and related services.



Name	Description	Status	Startup Type	Log On As
Symantec pcAnywh...	Allows Rem...	Started	Automatic	Local System
System Event Notifi...	Monitors s...	Started	Automatic	Local System
Task Scheduler	Enables a ...		Disabled	Local System
TCP/IP NetBIOS He...	Provides s...	Started	Automatic	Local Service
Telephony	Provides T...		Disabled	Local System
Telnet	Enables a r...		Disabled	Local Service
Terminal Services	Allows user...	Started	Manual	Local System

On the CallPilot at Site B, Set the Telephony Service to Automatic and start the service.



Name	Description	Status	Startup Type	Log On As
Symantec pcAnywh...	Allows Rem...	Started	Automatic	Local System
System Event Notifi...	Monitors s...	Started	Automatic	Local System
Task Scheduler	Enables a ...		Disabled	Local System
TCP/IP NetBIOS He...	Provides s...	Started	Automatic	Local Service
Telephony	Provides T...	Started	Automatic	Local System
Telnet	Enables a r...		Disabled	Local Service
Terminal Services	Allows user...	Started	Manual	Local System

Switchover Scenario #2: CCMS Recovery

To bring the original CCMS back online

- Fix the original issue
- When the original Active, primary CCMS is brought back on line, it needs first to be configured as a Standby connected to the New Active CCMS.
  For installation of AACC Application Redundancy please refer to Avaya Aura™ Contact Center Commissioning Guide (NN44400-312), Configuring Redundancy for Campus Co-resident server.
- Before switching over to the Original Active CCMS:
  - Manually de-acquire IVR and ACCESS ports of CallPilot 2 on CCMS B.
  - Disable and stop the Telephony service on CallPilot 2
  - On CallPilot 1 set the Telephony Service to Automatic and start up the server.
  - Perform a manual switchover to the original configuration.
  - Modify CCMS Server Configuration on CCMS A to connect to CallPilot 1
  - Normal operation will then be resumed. CCMS A will be able to route calls to all CC Agents and provide Voice services through CallPilot 1 only.

Configuration #2

CCMS GeoCampus with Geo Redundant CallPilot and replicated Mailboxes

Geographic Redundancy (GR) is supported on the following CallPilot servers:
1. 202i
2. 600r
3. 1005r
4. 1006r
5. 703t

Note: Geo Redundancy keycode must be purchased.
If Geo Redundancy is available in the keycode CPHA will not be available.

The systems will be configured as standalone CallPilots as in configuration #1.
CallPilot Geo Redundancy requires a keycode with this feature for both CallPilot servers. Refer to the "CallPilot Geographic Redundancy Application Guide" NN44200-322

The following steps are extracted from the CallPilot Geographic Redundancy Application Guide:
Each server should be joined to a domain with a Fully Qualified Domain Name (FQDN) that can be resolved from each CallPilot server; you must also configure both with "Voice Profile for Internet Messaging" (VPIM) as this is how the CallPilots will communicate.

On each CallPilot configure the following:
Under message delivery configuration -> Security Modes for SMTP Sessions:

- Enter a password for SMTP/VPIM (example 123213)
- User ID/Password Authentication is enabled

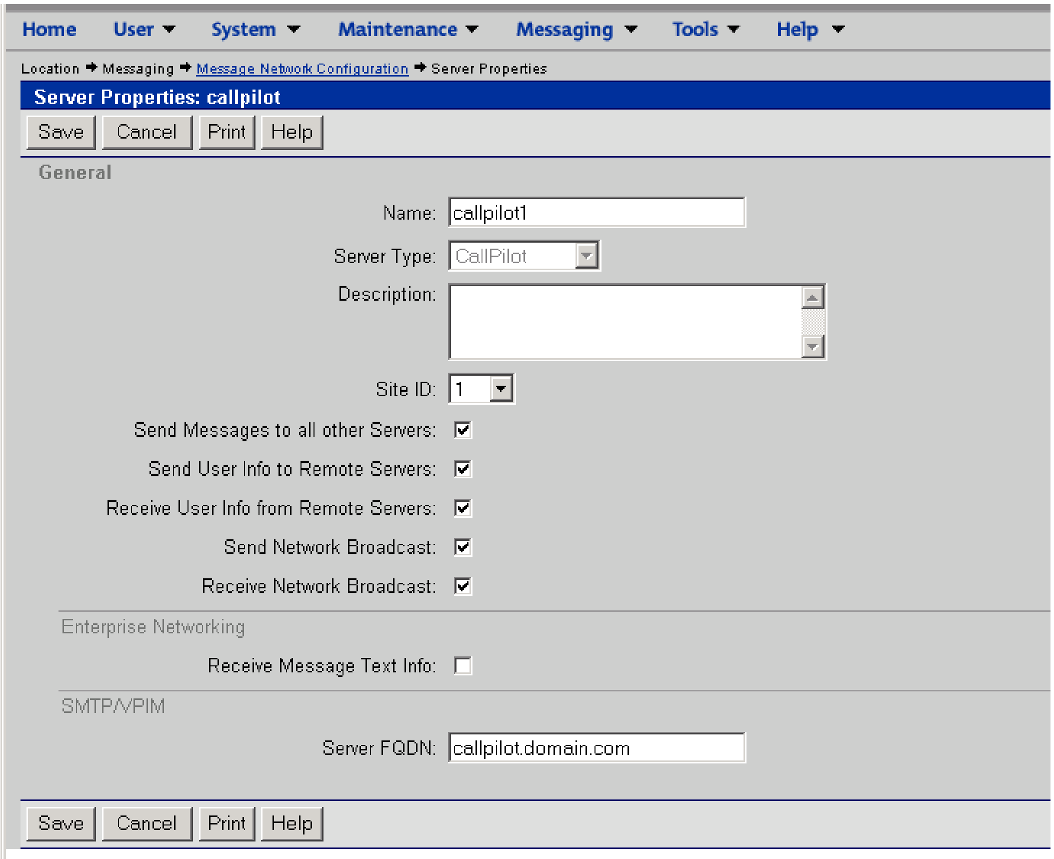
Under message network configuration:

- Server Properties (local and geo redundant)
    - Set the full FQDNs on both sites under networking config
    - Confirmed that the sites were configured with matching numbers
    - Set the general options to send / receive user info from Remote servers
- For the PRIME and geo redundant location properties:
    - CDP Dialing Plan for this Location
    - Mailbox Addressing Follows Dialing Plan
    - For CallPilot (1): CDP set to 61111 (Example), VPIM set to 61111 (Example)
    - For CallPilot (2): CPD set to 62222, VPIM set to 62222
    - Set the VPIM security server password to match what was entered earlier (123123)

Make sure the FQDN of both servers can ping in both directions.

From the CallPilot Manager launch Messaging / Message Network Configuration.

Under the Local Server Maintenance select the local CallPilot and click on “Show Details” Update the name, site ID, Select all the options to send and receive user info from remote servers and network broadcast, enter the FQDN and save.



Name: callpilot1

Server Type: CallPilot

Description:

Site ID: 1

Send Messages to all other Servers: ☑

Send User Info to Remote Servers: ☑

Receive User Info from Remote Servers: ☑

Send Network Broadcast: ☑

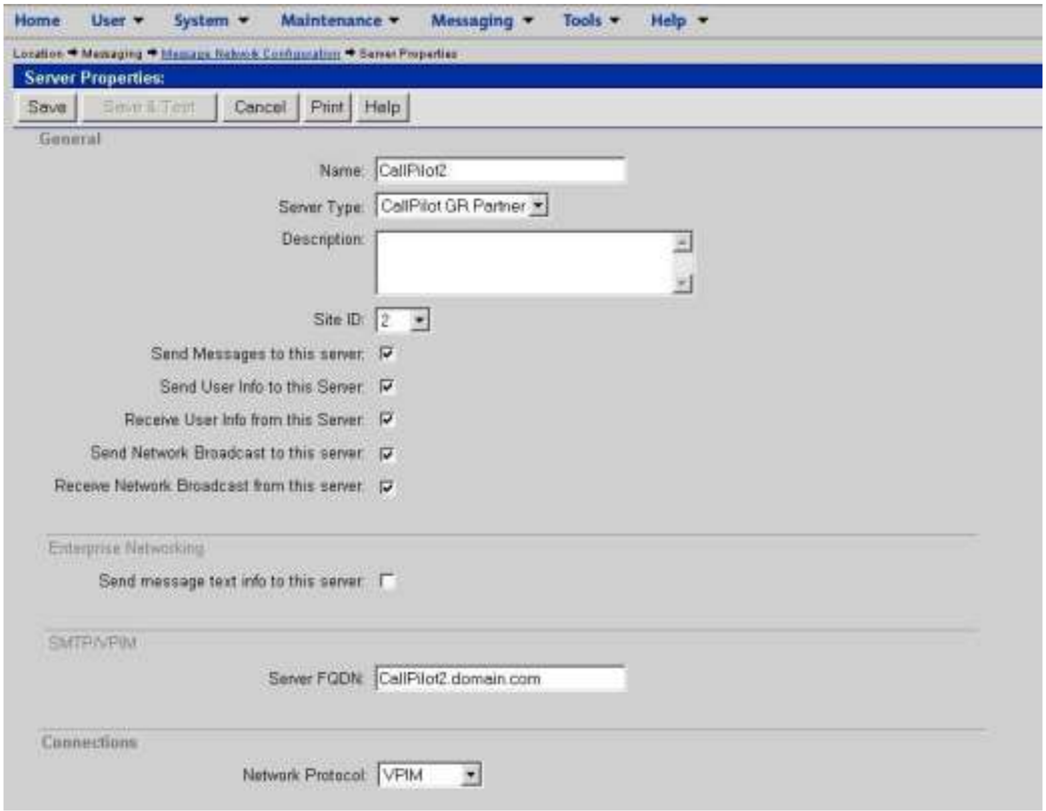
Receive Network Broadcast: ☑

Receive Message Text Info: ☐

Server FQDN: callpilot.domain.com

From the Message Network Configuration click on "New Server"
Enter the name of the Geo Site, enter a unique Site ID, Select the same checkboxes as the original CallPilot, the Network protocol is VPIM.

Under GR security enter a password, this will have to be the same on CallPilot 2 when you configure this side.



General

Name: CallPilot2

Server Type: CallPilot GR Partner

Description:

Site ID: 2

Send Messages to this server: ☑

Send User Info to this Server: ☑

Receive User Info from this Server: ☑

Send Network Broadcast to this server: ☑

Receive Network Broadcast from this server: ☑

Enterprise Networking

Send message text info to this server: ☐

SMTP/VPIM

Server FQDN: CallPilot2.domain.com

Connections

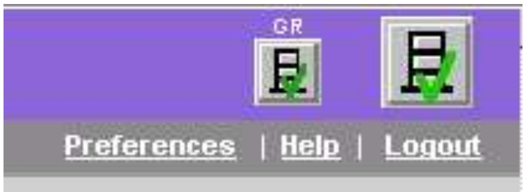
Network Protocol: VPIM

Repeat these steps on the second CallPilot setting it's local Site ID and FQDN to that configured for the Geo partner on site 1.

When these settings are completed you can check the status of the config by browsing to Messaging / Network Diagnostics.
Under the Network status choose Show Geo-Redundant servers, select the other CP and click "Compare with Selected".

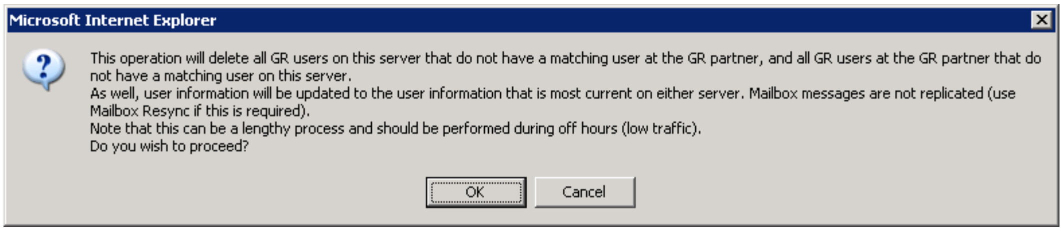
Resolve any issues reported and run the test tool again.

When CallPilot GR is fully up you will see the Icon in the top Right hand corner display a green checkbox:



Once the CallPilot GR partner is running you can now sync up the mailboxes.
First the users must be synced up.
This stage should be performed at an off peak time.

From the messaging menu choose Message Network configuration.
Select the Geo-redundant partner Server and press the "Sync GR Users" button
1. Log on to CallPilot Manager.
2. On the Messaging menu, choose Message Network Configuration.
3. Select the GR partner and click Sync GR users.
The Sync GR Users window opens in which you can choose the type of synchronization
4. Click Resync or Rebuild.
A warning displays asking for confirmation.
Be aware that all local GR users that do not have a matching user on the GR partner will be deleted, as well as GR users on the partner that are not present on the local server.



Microsoft Internet Explorer

This operation will delete all GR users on this server that do not have a matching user at the GR partner, and all GR users at the GR partner that do not have a matching user on this server.
As well, user information will be updated to the user information that is most current on either server. Mailbox messages are not replicated (use Mailbox Resync if this is required).
Note that this can be a lengthy process and should be performed during off hours (low traffic).
Do you wish to proceed?

5. Click OK.
6. You can monitor the status of the resynchronization

Once the users are synced the contents of the mailboxes are also resynchronized automatically when the user logs into their mailbox.

You may also manually resynchronize the mailboxes by performing the following steps
1. Log on to CallPilot Manager.
2. On the Maintenance menu, choose GR Manual Mailbox Resync.
3. Change search parameters as required and can click Search.
4. Select desired users and click Add to move those users over to the Selected Users List field.
5. Click Start Resync.
This replicates the mailbox information for the selected users.
The GR Status Resync window appears. Status will be updated as users are replicated.
6. You can monitor the status of the resynchronization.

For more information please refer to the documents:
NN44200-322_01.04_CallPilot_Geographic_Redundancy.pdf
Avaya Aura™ Contact Center Commissioning Guide (NN44400-312)

Appendix H T1/SMDI Expansion to High Capacity

Procedure to add two MPB96 boards and two T1 PCI cards

1. Courtesy stop all CallPilot channels.
2. Power down the server and all peripheral devices.
3. Disconnect the following cables:
    a) power cable
    b) peripheral device cable
    c) D/480JCT-2T1 cables
4. Remove the server cover.
5. Disconnect the CT Bus cable (if present).
6. Ensure that the current configuration is as follows (this is standard for a 96-channel configuration):
    a) There is an existing MPB96 board in PCI slot 3.
    b) There is an existing Intel D/480JCT-2T1 PCI card in slot 4, and its SW100 ID rotary dial switch is set to 0.
    c) There is an existing Intel D/480JCT-2T1 PCI card in slot 5, and its SW100 ID rotary dial switch is set to 1.
7. Remove any termination jumpers from the Intel D/480JCT-2T1 PCI cards. For jumper location, see Figure 35 on page 177.
8. Plug the first additional MPB96 card into PCI slot 6.
9. On the first additional Intel D/480JCT-2T1 PCI card:
    a) Set the card's SW100 ID rotary dial switch to 2.
    b) Ensure that there are no termination jumpers installed on P700.
    c) Plug the card into PCI slot 7.
10. On the second additional Intel D/480JCT-2T1 PCI card:
    a) Set the card's SW100 ID rotary dial switch to 3.
    b) Ensure that there are no termination jumpers on P700 pins 3 and 4.
    c) Plug the card into PCI slot 8.
11. Plug the second additional MPB96 card into PCI slot 9.
12. Connect the 7 drop CT Bus cable to ensure that the connectors are connected to the end cards and no connector is left dangling at any end of the cable.
13. Replace the server cover.
14. Replace the front bezel and lock it.
15. Reconnect the peripheral device and power cables.
16. Connect the D/480JCT-2T1 cables to the two new and two existing Intel D/480JCT-2T1 PCI cards.
17. Power up the server and log on to Windows.

Result: The Windows New Hardware Found Wizard screen appears.

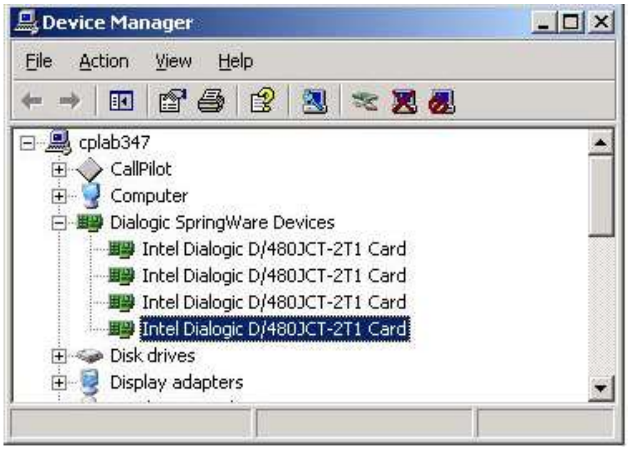
ATTENTION

*Before clicking Next to install the hardware driver, wait 10 minutes or until you see the dialog box "****CallPilot is running and is able to accept calls****" otherwise the server could display a blue screen and then restart. If this happens, the server may not recognize the installed cards and boards.*

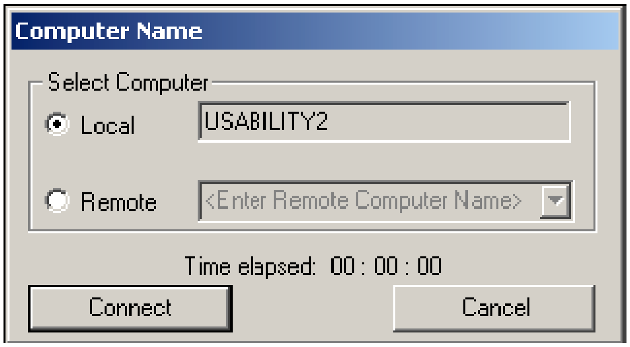
18. Wait 10 minutes or until you see the dialog box "CallPilot is running and is able to accept calls"

ATTENTION
Failure to adhere to step 18 could result in a blue-screen followed by server restart. If this happens, the server may not recognize the installed cards and boards. Wait 10 minutes for the server to return to full service.

19. Click Next on the New Hardware Found Wizard Screen.
20. Select the presented Avaya MPB driver and click Next.
21. Repeat the previous two steps each time the Windows New Hardware Found Wizard screen appears.
22. In Windows Desktop right-click to **My Computer**, select **Properties**, go to **Hardware** tab, open **Device Manager**, expand **Dialogic SpringWare Devices** item. Verify the Device Manager main window contains a tree structure of the boards installed in your system.


Device Manager
File
Action
View
Help
cplab347
CallPilot
Computer
Dialogic SpringWare Devices
Intel Dialogic D/480JCT-2T1 Card
Intel Dialogic D/480JCT-2T1 Card
Intel Dialogic D/480JCT-2T1 Card
Intel Dialogic D/480JCT-2T1 Card
Disk drives
Display adapters

23. The next step is to detect and start the board using the Dialogic Configuration Manager (DCM). DCM is what actually makes the board function; if the board isn't started in DCM it will not work in the telephony application.
24. From the Windows **Start** menu, select **Programs > Intel Dialogic System Software > Configuration Manager-DCM** to launch the configuration manager (DCM).The Computer Name dialog box will appear:

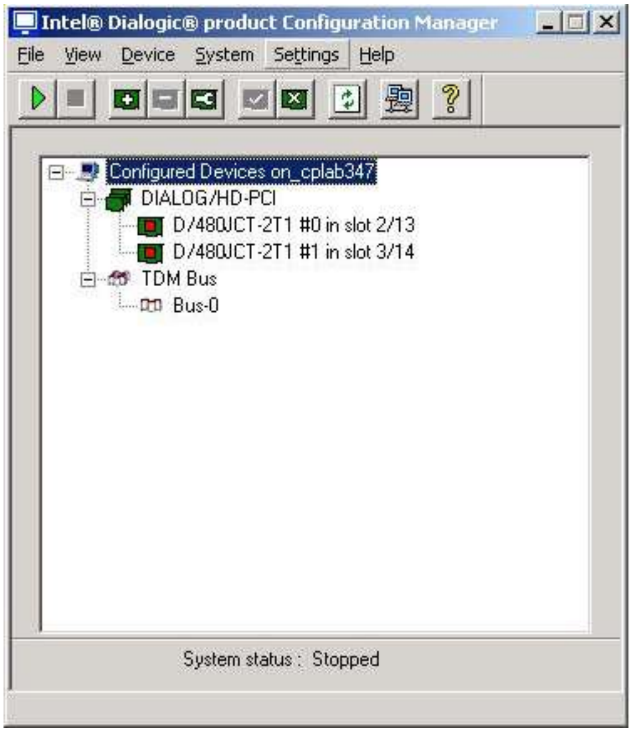


USABILITY2

Time elapsed: 00 : 00 : 00

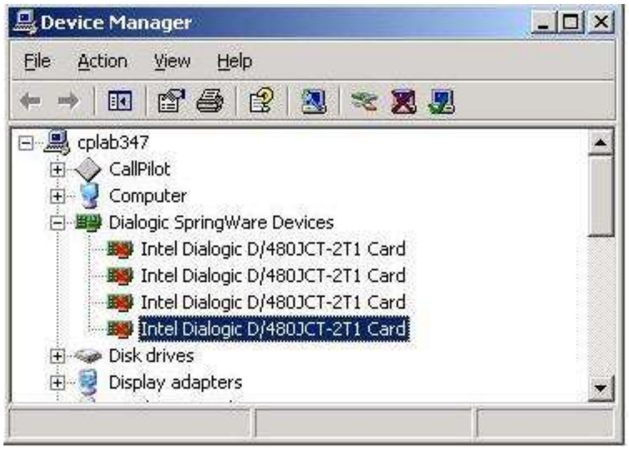
Note: The Computer Name dialog box displays automatically the first time you run the DCM with the local computer name as the default. It will not appear on subsequent launches of DCM.

25. Connect to the local computer by clicking **Connect**
26. After connecting to a computer, you will see a message that indicates that boards are being detected, and then the DCM main window. Verify the DCM main window contains a tree structure of the boards installed in your system.

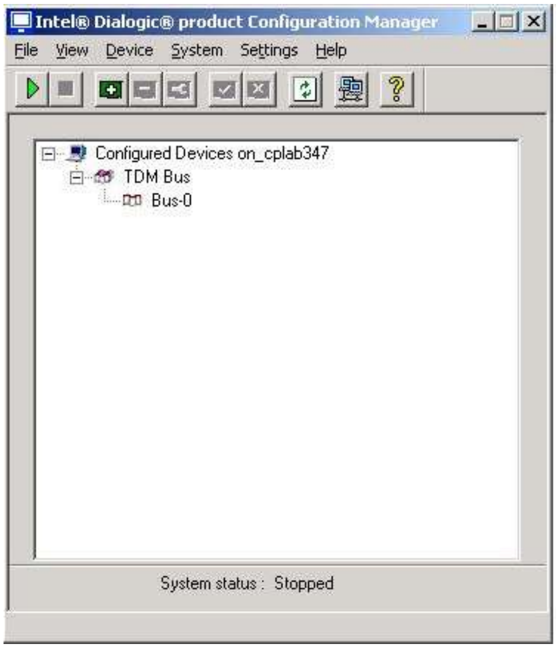


Intel® Dialogic® product Configuration Manager
File View Device System Settings Help
Configured Devices on_cplab347
DIALOG/HD-PCI
D/480JCT-2T1 #0 in slot 2/13
D/480JCT-2T1 #1 in slot 3/14
TDM Bus
Bus-0
System status : Stopped

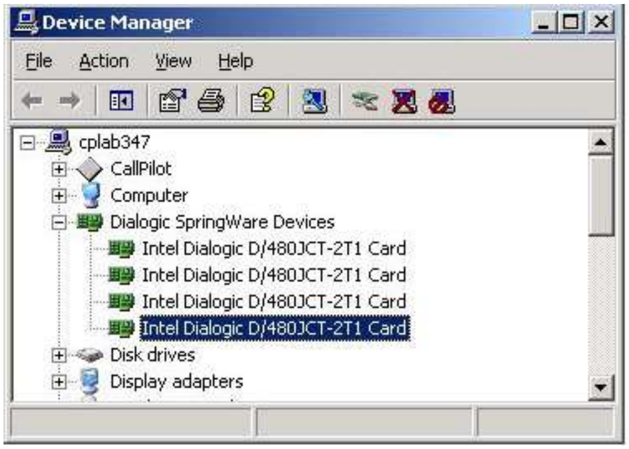
27. If the number of Dialogic boards displayed in the DCM window matches the number of installed boards skip to step **36**. in the DCM windows you see that not all boards installed in your system are detected, go to step 28, otherwise go to step 33Otherwise proceed to step **28**.
28. From the Windows **Start** menu, select **Settings > Control Panel > Administrative Tools > Services**. The Services Applet is displayed. In this Applet, right click on the "CallPilot HAL Monitor Service", and select "Stop". Do the same for "Intel Dialogic Product System Service" from Services Applet Panel, stop CallPilot HAL Monitor service and Intel Dialogic Product System Service if started. This step can be ignored if these two services have not been started. The Applet "Status" column displays whether or not the service has been started.
29. From Device Manager disable all boards installed in your system. From the Windows **Start** menu, select **Programs > Administrative Tools > Computer Management.** On the left hand side of the Computer Management window select **Device Manager**. On the right hand side click the plus sign next to **Dialogic Springware Devices** (all 4 Dialogic boards should appear). Starting with the top board, right click and select "Disable" for each of the 4 Dialogic boards. If you are prompted to reboot, select **No** and continue to disable Dialogic boards until all 4 have been disabled. Note that not all boards may display a strikethrough **X** once the board has been disabled.


Device Manager
File Action View Help
cplab347
CallPilot
Computer
Dialogic SpringWare Devices
Intel Dialogic D/480JCT-2T1 Card
Intel Dialogic D/480JCT-2T1 Card
Intel Dialogic D/480JCT-2T1 Card
Intel Dialogic D/480JCT-2T1 Card
Disk drives
Display adapters

30. Restart the server.
31. **NOTE:** If you are prompted to reboot, select **No** and continue to disable Dialogic boards until all 4 have been disabled. Note that all boards may not display a strikethrough **X** once the board has been disabled. To actually disable the boards, restart the server. Log in to Windows.
32. The Maintenance Configuration Detection Information window appears. Click “OK”. Wait until the startup diagnostics have finished.
33. From Services Applet Panel, stop CallPilot HAL Monitor service and Intel Dialogic Product System Service (if they are started). Refer to Step **27** for directions on stopping services, if necessary. Launch Device Manager and Dialogic Configuration Manager. Go to step 30 to continue the upgrade procedure.
34. Re-launch DCM (refer to step **23** for directions, if necessary). From the DCM main windows, click **Settings > Auto detect devices**. You will see a message that indicates that boards are being detected, and then the DCM main window. You should see a screen similar to the following. Verify the DCM main window contains an empty tree structure of the boards installed in your system:

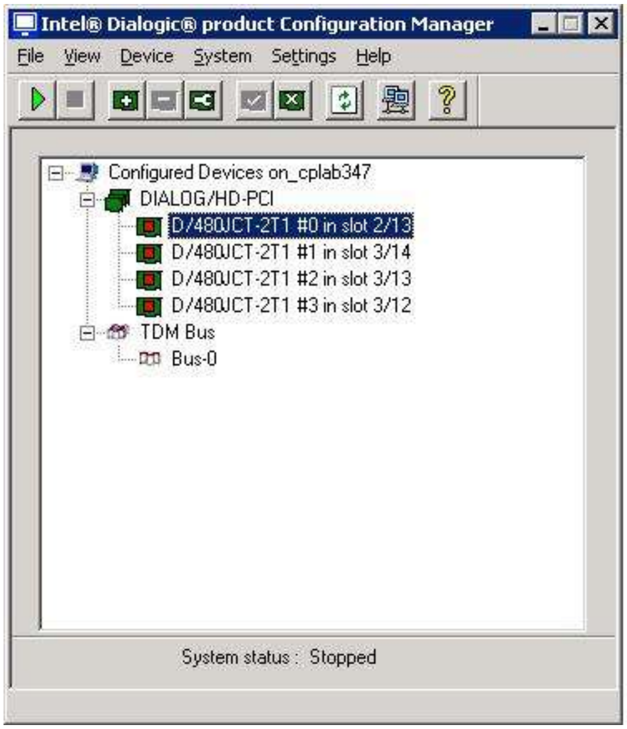

Intel® Dialogic® product Configuration Manager
File View Device System Settings Help
Configured Devices on_cplab347
TDM Bus
Bus-0
System status : Stopped

35. Minimize DCM and bring Computer Management back up by selecting **Start > Programs > Administrative Tools > Computer Management**. On the left hand side of the Computer Management window select **Device Manager**. On the right hand side click the plus sign next to **Dialogic Springware Devices** (all 4 Dialogic boards should appear as disabled). Starting with the top board, right click and select "Enable" for each of the 4 Dialogic boards. From Device Manager, enable all boards installed in your system.



- cplab347
  - CallPilot
  - Computer
  - Dialogic SpringWare Devices
    - Intel Dialogic D/480JCT-2T1 Card
    - Intel Dialogic D/480JCT-2T1 Card
    - Intel Dialogic D/480JCT-2T1 Card
    - Intel Dialogic D/480JCT-2T1 Card
  - Disk drives
  - Display adapters

36. Bring the DCM window back up and From the DCM main windows, click **Settings > Auto detect devices**. You will see a message that indicates that boards are being detected, and then the DCM main window. Verify the DCM main window contains a tree structure of the boards installed in your system.



- Configured Devices on_cplab347
  - DIALOG/HD-PCI
    - D/480JCT-2T1 #0 in slot 2/13
    - D/480JCT-2T1 #1 in slot 3/14
    - D/480JCT-2T1 #2 in slot 3/13
    - D/480JCT-2T1 #3 in slot 3/12
  - TDM Bus
    - Bus-0

System status : Stopped

37. Close DCM and Device Manager; restart the server.
38. Once the server has restarted you receive the Maintenance Configuration Detection Information dialog box a dialog box indicating you have new hardware. Click OK.
39. Wait for the startup diagnostics to finish and then run the Configuration Wizard to configure the new hardware. Run the Configuration Wizard to configure the new hardware. For instructions, refer to the Installation and Configuration Task List (555-7101-210).