



Avaya CallPilot® Communication Server 1000 and Avaya CallPilot Server Configuration

5.0
NN44200-312, 01.12
December 2010

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Copyright

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

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Customer service	9
Getting technical documentation	9
Getting product training	9
Getting help from a distributor or reseller	9
Getting technical support from the Avaya Web site	10
Chapter 2: Avaya CallPilot® and Avaya CS 1000 connectivity overview	11
In this chapter	11
Overview	12
Introduction	12
Customer Documentation Map	12
Before you begin	15
Installation and configuration checklist	15
Contact Center Voice Services Support	17
Introduction	17
Configuring the CS 1000 system to support CallPilot and Contact Center Server	18
Configuring CallPilot for Contact Center Voice Services Support	18
See also	19
Section A: CallPilot network setup	19
In this section	19
CallPilot and CS 1000 integration	19
Introduction	19
Sample network diagrams	20
201i or 202i server	20
Tower or rackmount servers	22
CS 1000 network setup	22
CallPilot components	23
CallPilot server	23
MGate card (NTRB18CA or NTRB18DAE5) -- tower and rackmount servers only	23
MPB boards (for tower and rackmount servers only)	23
MPC-8 cards	24
Modem	24
Desktop client PCs	24
CS 1000 Media Gateway	24
Introduction	24
Media Gateway and Media Gateway Expansion	25
Section B: Understanding call routing	26
In this section	26
CS 1000 call routing components	26
Introduction	26
Automatic Call Distribution	26
How CallPilot uses ACD virtual agents	27
Control Directory Number	27
How CallPilot uses CDNs	27
Call queuing	28
Call routing	28
See also	28
Phantom DNSs	28

Introduction.....	28
Creating a Phantom DN.....	29
Phantom DN's forward to a CDN queue.....	29
Services that should use phantom DN's.....	29
Networking services.....	30
Example.....	30
CallPilot Service Directory Numbers and the SDN Table.....	30
Introduction.....	30
What is the SDN Table?.....	31
What the SDN Table controls.....	31
Types of SDN's.....	31
Inbound SDN's require DN's on the CS 1000 system.....	31
Outbound SDN's do not require DN's on the CS 1000 system.....	32
How calls are routed.....	33
Example of phantom DN or dummy ACD DN usage.....	34
What happens when users dial the service DN's.....	35
Multimedia channels in the CallPilot server.....	35
Multimedia Processing Units.....	35
Types of multimedia channels.....	35
How multimedia channels are acquired by callers.....	36
Introduction.....	36
What happens when the call is answered.....	36
What happens when the call is dropped.....	37
What is next?.....	37

Chapter 3: Connecting the Avaya CallPilot® server to the Avaya Communication Server 1000 system.....39

In this chapter.....	39
Section A: Installing the MGate card.....	39
In this section.....	39
About the MGate card (NTRB18CA or NTRB18DAE5).....	40
Introduction.....	40
Number of channels supported.....	41
LED indicators.....	41
Impact of a faulty MGate card (NTRB18CA or NTRB18DAE5).....	42
Required components.....	43
Installing the MGate card (NTRB18CA or NTRB18DAE5).....	45
Introduction.....	45
Before you begin.....	45
MGate Card (NTRB18CA) DIP switches.....	46
What is next?.....	48
Replacing an MGate card (NTRB18CA or NTRB18DAE5).....	48
Introduction.....	48
To replace an MGate card.....	49
Section B: Connecting the CallPilot server to the switch.....	50
In this section.....	50
About the MGate cables.....	51
Introduction.....	51
DS30X cables supported by MPB16-4 boards.....	52
DS30X cable supported by the NTRH40AA MPB96 board.....	53
Cables supported by the NTRH40CAE5 MPB96 board.....	54

Connecting MPB16-4 boards to MGate cards (NTRB18CA or NTRB18DAE5).....	55
Introduction.....	55
Cabling diagrams.....	55
Identifying the location of MPB 1 and MPB 2.....	56
Identifying the location of MGate 1, 2, and 3.....	56
One MPB16-4 board and one MGate card (32 channels or less).....	56
Two MPB16-4 boards and one MGate card (32 channels or less).....	57
One MPB16-4 board and two MGate cards (48 channels or less).....	58
Two MPB16-4 boards and two MGate cards (48 channels or less).....	58
To connect the DS30X cable.....	59
What is next?.....	60
Connecting the MPB96 boards to MGate cards (NTRB18CA or NTRB18DAE5).....	61
Introduction.....	61
MGate cabling to the NTRB18DAE5 MPB96 card (703t, 1002rp, 600r, 1005r).....	62
High capacity configuration.....	63
MGate cabling to the NTRH40CAE5 MPB96 card (600r, 1005r, and 1006r).....	65
High capacity configuration.....	66
NTRB18DAE5 MGate Link LED indications.....	68
What is next?.....	70

Chapter 4: Configuring the Avaya Communication Server 1000 system.....71

In this chapter.....	71
Avaya CS 1000 hardware and software requirements.....	72
Required hardware.....	72
Required CS 1000 system software.....	72
Required X21 PEPs.....	72
CS 1000 configuration checklist.....	73
Introduction.....	73
How the overlays are presented in this chapter.....	75
Working with overlays.....	76
The customer number.....	76
Provisioning the ELAN subnet.....	76
Introduction.....	76
Defining the Message Register for AML message tracing.....	78
Introduction.....	78
Configuring CS 1000 IP addresses and enabling the Ethernet interface.....	79
Introduction.....	79
To configure the IP addresses and enable the Ethernet interface.....	79
Defining CallPilot in the customer data block.....	82
Introduction.....	82
Additional steps to support the Call Forward by Call Type feature.....	85
Configuring the ACD agent queue.....	86
Introduction.....	86
Contact Center Voice Services Support additional requirements.....	86
Configuring ACD agents.....	87
Introduction.....	87
Terminal numbers.....	87
Integrated server (201i or 202i server).....	87
Tower or rackmount servers.....	88
Position IDs.....	88
Enabling the card slots.....	89

Introduction.....	89
To enable the card slots.....	90
Defining the default ACD DN.....	90
Introduction.....	90
Configuring CDN queues for messaging services.....	91
Introduction.....	91
Configuring phantom DNS.....	92
Introduction.....	92
Supporting multiple languages.....	93
Virtual fax DNS for users with fax capabilities.....	93
To check for existing phantom loops.....	94
Configuring dummy ACD DNS.....	96
Introduction.....	96
Example.....	96
Provisioning user phonesets.....	97
Introduction.....	97
Required features.....	97
Configuring the route data block for Network Message Service.....	100
Introduction.....	100
Saving CS 1000 changes.....	101
Introduction.....	101
What is next?.....	101

Chapter 5: Configuring the Avaya CallPilot® server software.....103

In this chapter.....	103
Overview.....	103
Introduction.....	103
Plan your responses to the Configuration Wizard.....	104
Online Help for the Configuration Wizard.....	104
Running the Configuration Wizard to detect replacement boards.....	104
Logging on to Windows 2003 on the CallPilot server.....	105
Introduction.....	105
Running the Setup Wizard.....	106
Logging on to the CallPilot server with CallPilot Manager.....	107
Introduction.....	107
Logon process overview.....	107
Relationship of the CallPilot Manager web server to the CallPilot server.....	108
Running the Configuration Wizard.....	111
Introduction.....	111
Requirements.....	111
Considerations on configuring STI links for the CallPilot tower and rackmount servers.....	113
What is next?.....	114
Changing pcAnywhere caller passwords.....	114
Introduction.....	114
What is Next?.....	115
Setting Remote Desktop Policy on a Server.....	115
What is Next?.....	117
Configuring CallPilot to operate in a Windows 2000 or 2003 domain.....	118
Introduction.....	118
To set domain group policy.....	118
To add CallPilot server to a domain.....	119

To stop and disable the Win32 Time Service.....	123
To set up user accounts for remote access domain.....	124
Option 1: Use the local Administrator account for remote logon.....	126
Option 2: Use the Domain user account for remote logon.....	126
To run Configuration Wizard in a domain.....	127
To change the computer name.....	127
To change the local account passwords.....	127
What is next?.....	128
Chapter 6: Testing the Avaya CallPilot® installation.....	129
In this chapter.....	129
Checking that Avaya CallPilot is ready to accept calls.....	129
Introduction.....	129
Checking system readiness by observing the dialog box messages.....	130
Alternative methods for verifying that CallPilot is ready to accept calls.....	132
View events in CallPilot Manager or in the operating system Event Viewer on the server.....	132
Observe the HEX display (for the 201i or 202i server only).....	132
Testing the connection to the ELAN subnet.....	133
Introduction.....	133
Testing the connection to the NNS Subnet.....	134
Introduction.....	134
Verifying that CallPilot can receive calls.....	135
Introduction.....	135
What is next?.....	135
Testing the CallPilot software and channels.....	136
Introduction.....	136
Before you begin.....	136
To verify that you can leave a message.....	136
To configure the Voice Messaging DN.....	137
Verifying that each call channel and multimedia channel is functioning properly.....	140
To test call channels and voice channels.....	141
To test call channels and fax channels.....	142
What is next?.....	146
Chapter 7: Avaya CallPilot® 5.0 ELAN IPsec.....	147
Overview.....	147
ELAN IPsec requirements.....	147
Information required for configuring IPsec.....	148
IPsec configuration overview.....	148
Configuring IPsec on your CallPilot server.....	149
Creating a custom IPsec MMC console.....	149
Creating and configuring IPsec policy.....	150
Starting the Windows IPsec Services.....	156
Assigning ELAN IPsec Policy to your CallPilot server.....	156
Unassigning the CallPilot ELAN IPsec Policy.....	157
Troubleshooting.....	158
Printing IPsec policy parameters.....	158
Index.....	163

Chapter 1: Customer service

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

Navigation

- [Getting technical documentation](#) on page 9
- [Getting product training](#) on page 9
- [Getting help from a distributor or reseller](#) on page 9
- [Getting technical support from the Avaya Web site](#) on page 10

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

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

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

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

Chapter 2: Avaya CallPilot® and Avaya CS 1000 connectivity overview

In this chapter

[Overview](#) on page 12

[Contact Center Voice Services Support](#) on page 17

[Section A: CallPilot network setup](#) on page 19

[CallPilot and CS 1000 integration](#) on page 19

[CS 1000 Media Gateway](#) on page 24

[Section B: Understanding call routing](#) on page 26

[CS 1000 call routing components](#) on page 26

[Phantom DNs](#) on page 28

[CallPilot Service Directory Numbers and the SDN Table](#) on page 30

[How calls are routed](#) on page 33

[Multimedia channels in the CallPilot server](#) on page 35

[How multimedia channels are acquired by callers](#) on page 36

Overview

Introduction

This guide describes the Communication Server 1000 (CS* 1000) system setup and Avaya CallPilot* server configuration steps of the CallPilot installation. This guide includes:

- configuring the CS 1000 system for correct operation with CallPilot
- connecting the CallPilot system to the CS 1000 system and the Avaya Server Subnet (NS Subnet)
- configuring the CallPilot server

Customer Documentation Map

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

Table 1: CallPilot Customer Documentation Map

Fundamentals
Avaya CallPilot® Fundamentals Guide (NN44200-100)
Avaya CallPilot® Library Listing (NN44200-117)
Planning and Engineering
Avaya CallPilot® Planning and Engineering Guide (NN44200-200)
Avaya CallPilot® Network Planning Guide (NN44200-201)
Avaya Communication Server 1000 Converging the Data Network with VoIP Fundamentals (NN43001-260)
Solution Integration Guide for Avaya Communication Server 1000/CallPilot®/NES Contact Center/Telephony Manager (NN49000-300)
Installation and Configuration
Avaya CallPilot® Upgrade and Platform Migration Guide (NN44200-400)
Avaya CallPilot® High Availability: Installation and Configuration (NN44200-311)
Avaya CallPilot® Geographic Redundancy Application Guide (NN44200-322)

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

Avaya CallPilot® Quickstart Guide (NN44200-313)

Avaya CallPilot® Installer Roadmap (NN44200-314)

Server Installation Guides

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

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

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

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

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

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

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

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

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

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

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

Configuration and Testing Guides

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

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

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

Unified Messaging Software Installation

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

Administration

Avaya CallPilot® Administrator Guide (NN44200-601)

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

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

Avaya CallPilot® Application Builder Guide (NN44200-102)

Avaya CallPilot® Reporter Guide (NN44200-603)

Maintenance

Avaya CallPilot® Troubleshooting Reference Guide (NN44200-700)

Avaya CallPilot® Preventative Maintenance Guide (NN44200-505)

Server Maintenance and Diagnostics

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

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

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

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

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

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

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

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

End User Information

End User Cards

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Before you begin

Before configuring the CS 1000 system and CallPilot server:

- Review the Installing CallPilot section in the CallPilot Installation and Configuration Task List.
- Complete stage 2 of the CallPilot Installation and Configuration Task List.
- Complete the worksheets in the CallPilot Installation and Configuration Task List.

 **Note:**

If you need a high-level overview of CallPilot and CS 1000 connectivity, then read the remainder of this chapter.

Otherwise, the installation steps begin in the following chapters:

- for tower or rackmount servers, in [Connecting the Avaya CallPilot® server to the Avaya Communication Server 1000 system](#) on page 39
- for the 201i or 202i server, in [Configuring the Avaya Communication Server 1000 system](#) on page 71

Complete the steps in each chapter before you continue to the next chapter.

Installation and configuration checklist

Check off the stages and steps in [Table 2: Installation and configuration checklist](#) on page 16 as they are completed.

Table 2: Installation and configuration checklist

Step	Description	Check
Stage 1: Install the connectivity hardware.		
<p> Note: For the 201i or 202i server, this stage is not applicable. Hardware connectivity is established when the 201 or 202i server is installed in the CS 1000 system, as described in the CallPilot <server_model> Server Hardware Installation Guide.</p>		
1	If your server is a tower or rackmount server, install the MGate card (NTRB18CA or NTRB18DAE5) in the CS 1000 system. For instructions, see Installing the MGate card (NTRB18CA or NTRB18DAE5) on page 45.	<input type="checkbox"/>
2	Connect the tower or rackmount server to the CS 1000 system. For instructions, see Section B: Connecting the CallPilot server to the switch on page 50.	<input type="checkbox"/>
Stage 2: Configure the CS 1000 system and CallPilot server.		
3	Configure the CS 1000 system. Use the "Switch configuration worksheet" that you completed in the CallPilot Installation and Configuration Task List. For configuration instructions, see CS 1000 configuration checklist on page 73.	<input type="checkbox"/>
4	Run the Configuration Wizard and configure the CallPilot server. Use the "Configuration Wizard worksheet" that you completed in the CallPilot Installation and Configuration Task List. For configuration instructions, see Running the Configuration Wizard on page 111.	<input type="checkbox"/>
5	<p>Change the pcAnywhere password or set the Remote Desktop Policy.</p> <ul style="list-style-type: none"> • If you are using pcAnywhere, continue to Changing pcAnywhere caller passwords on page 114. • If you are using Remote Desktop Connection, continue to Setting Remote Desktop Policy on a Server on page 115. 	<input type="checkbox"/>
Stage 3: Test CallPilot connectivity.		
<p> Note: For instructions, see Testing the Avaya CallPilot® installation on page 129.</p>		
6	Check the CallPilot system-ready indicators to see if CallPilot is ready to accept calls.	<input type="checkbox"/>
7	Test the connection to the ELAN subnet, if applicable.	<input type="checkbox"/>
8	Test the connection to the Avaya Server Subnet (NS Subnet).	<input type="checkbox"/>
9	Verify that CallPilot answers when you dial the Voice Messaging DN.	<input type="checkbox"/>

Step	Description	Check
Stage 4: Test the CallPilot services and channels.		
	 Note: For instructions, see Testing the Avaya CallPilot® installation on page 129.	
10	Check the system-ready indicators.	<input type="checkbox"/>
11	Verify network connectivity to the CallPilot server over the ELAN subnet and NNS Subnet.	<input type="checkbox"/>
12	Verify that CallPilot can receive calls.	<input type="checkbox"/>
13	Verify that you can leave a message.	<input type="checkbox"/>
14	Verify that you can retrieve a message.	<input type="checkbox"/>
15	Verify that each call channel and multimedia channel is functioning correctly.	<input type="checkbox"/>
16	Check for CallPilot alarms using the Alarm Monitor in CallPilot Manager. Upon confirmation that CallPilot is operating correctly, clear all alarms.	<input type="checkbox"/>
Stage 5: Install CallPilot Manager on a stand-alone web server (optional).		
17	Perform this step only if you want to set up a separate web server for CallPilot administration. This is necessary if you want to use the Reporter application, or if high administration traffic is expected. For instructions, see the CallPilot Software Administration Guide.	<input type="checkbox"/>

Contact Center Voice Services Support

Introduction

This section is applicable only if you are enabling the Contact Center* Voice Services Support feature. This section provides an overview of the specific CS 1000 configuration steps required for the Contact Center Voice Services Support feature.

Notes:

For Contact Center integration with CallPilot, Contact Center channels can only be voice channels.

ACD overflow is not supported.

Configuring the CS 1000 system to support CallPilot and Contact Center Server

This guide provides the specific CS 1000 system configuration instructions required to support CallPilot. Where there is an exception or additional step required for the Contact Center Voice Services Support feature, this information is also provided. A list of these exceptions and additional steps is provided below:

1. In overlay 17 (see [Provisioning the ELAN subnet](#) on page 76), the SECU prompt must be set to YES.
2. You must set up two additional ACD agent queues: one for ACCESS ports, and one for IVR* ports. See [Configuring the ACD agent queue](#) on page 86.
3. In overlay 11, you must specify AST 0 1, where 0 is the number for key 0, and 1 is the number for key 1.

Configuring CallPilot for Contact Center Voice Services Support

To configure CallPilot for Contact Center Voice Services Support, make the following changes.

1. In the Configuration Wizard, you must specify the following information for the Contact Center Voice Services Support feature:
 - On the CS 1000 Information web page, you must specify the Contact Center Server NNS Subnet IP address.
 - In the Channel Detail Information dialog box, you must select the check box for ACCESS or IVR for channels that are to be used for the Contact Center Voice Services Support feature. These are the same channels that you must program on the CS 1000 system in an ACCESS ACD queue or IVR ACD queue. Also specify the Class ID for the channel.
2. In the CallPilot Manager Service Directory Number page, do the following:
 - Use the ACCESS ACD-DN to create an SDN for the Contact Center Voice Services Support feature.
 - Define treatment IDs used by Contact Center Server as voice menus or announcements.

See also

See the Contact Center Server documentation for additional CS 1000 system instructions related to Contact Center Server configuration.

For additional information on Contact Center to CallPilot integration, see the CallPilot Distributor Technical Reference.

Section A: CallPilot network setup

In this section

[CallPilot and CS 1000 integration](#) on page 19

[CS 1000 Media Gateway](#) on page 24

CallPilot and CS 1000 integration

Introduction

This section describes how the CallPilot server is integrated into your network with the CS 1000 system.

Sample network diagrams

201i or 202i server

[Figure 1: 201i integrated with CS 1000](#) on page 21 shows an example of how the 201i server can be integrated with the CS 1000 system in your network.

[Figure 2: 202i integrated with CS 1000](#) on page 21 shows an example of how the 202i server can be integrated with the CS 1000 system in your network.

* Notes

1. Media Gateway or Media Gateway expansion can be used.
2. CallPilot Server represents 201i CallPilot Server, which is an internal card.

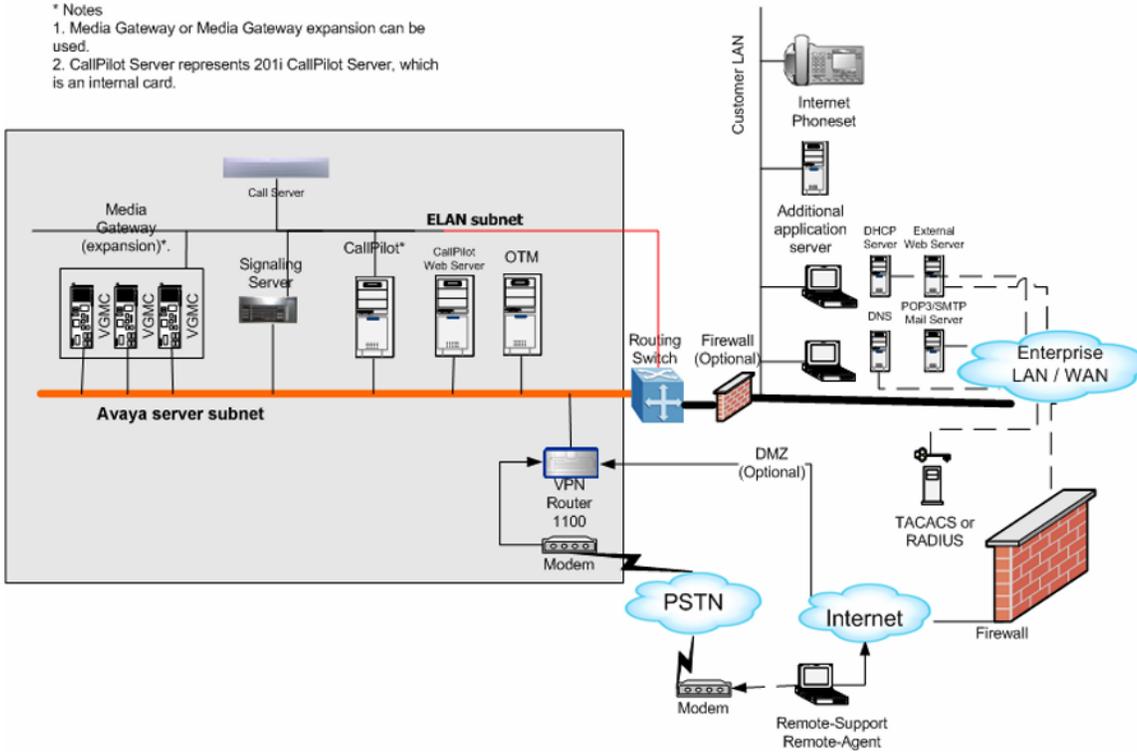


Figure 1: 201i integrated with CS 1000

Note*: Media Gateway Expansion cabinet can only be used with CP 202i.

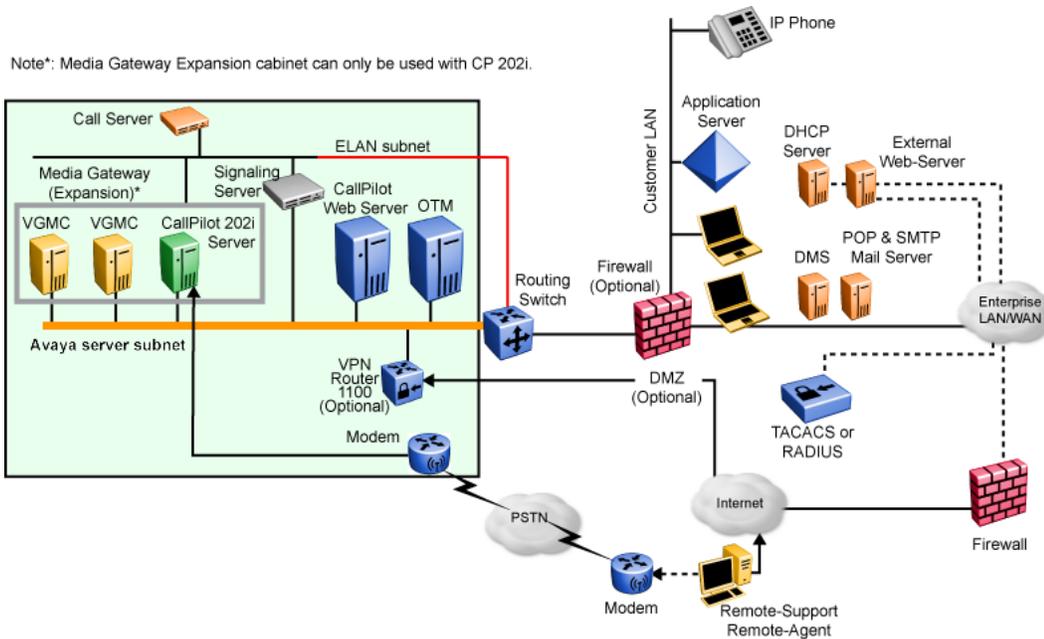


Figure 2: 202i integrated with CS 1000

Tower or rackmount servers

[Figure 3: Tower/rackmount server integrated with CS 1000](#) on page 22 shows how a tower or rackmount server (for example, 703t, or 1002rp) can be integrated with the CS 1000 system in your network:

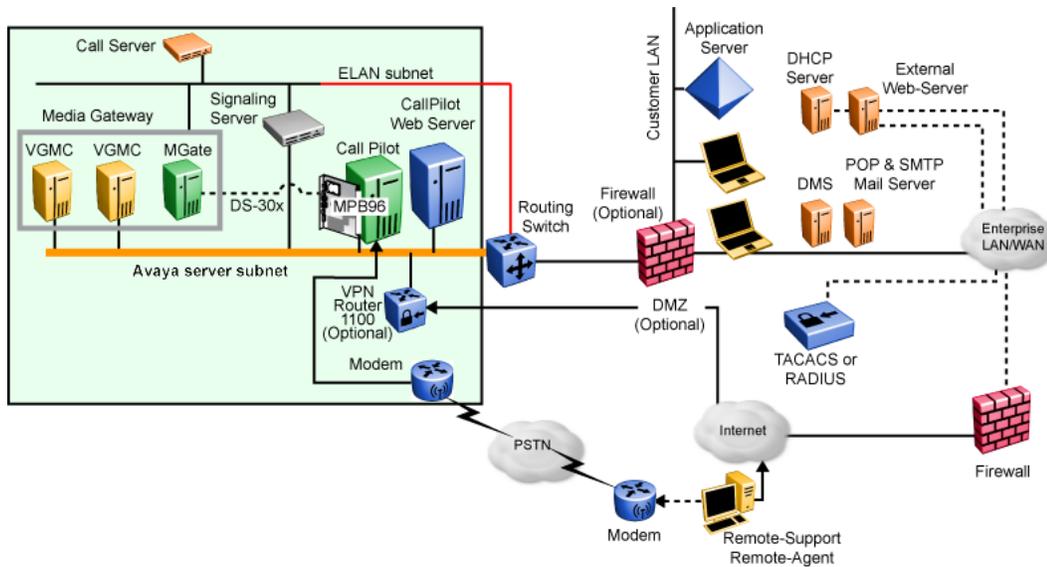


Figure 3: Tower/rackmount server integrated with CS 1000

*** Note:**

The above diagram shows a tower server. However, the same configuration applies to a rackmount server.

CS 1000 network setup

In the previous illustrations, the telephony LAN (TLAN) provides IP connectivity between the CS 1000 system and the i2004 Internet phonesets. The connection between the Call Server and Media Gateway can be point-to-point, or it can be through the LAN, if the system is installed in a distributed data network.

For information about the CS 1000 system and i2004 Internet phoneset bandwidth and network requirements, see the Communication Server 1000S: Installation and Configuration

For a description of each CS 1000 system component, see [CS 1000 Media Gateway](#) on page 24.

CallPilot components

CallPilot server

The CallPilot server connects to the CS 1000 system and, where desktop messaging is enabled, to the Avaya Server Subnet (NS Subnet). If your server is a 201 or 202i server, it resides inside the CS 1000 system.

MGate card (NTRB18CA or NTRB18DAE5) -- tower and rackmount servers only

The MGate card (NTRB18CA or NTRB18DAE5) is a line card that is installed inside the CS 1000 system. The MGate card sends the voice and data signals to the MPB boards in the CallPilot server.

MPB boards (for tower and rackmount servers only)

The CallPilot server is equipped with one of the following types of MPB boards:

- MPB16-4 boards

DSPs are provided on the MPB16-4 board in the form of two integrated MPCs and up to four optional MPC-8 cards. (For more information about MPC-8 cards, see [MPC-8 cards](#) on page 24.)

MPB 16-4 boards are no longer shipped with the CallPilot server. The MPB96 supersedes the MPB16-4.

- MPB96 boards

DSPs are provided on the MPB96 board in the form of 12 integrated MPCs. MPC-8 cards are not required on the MPB96 board.

Each tower or rackmount CallPilot server ships with at least one MPB96 board.

MPC-8 cards

The MPC-8 cards reside in slots in the 201i server, or in the MPB16-4 board for tower or rackmount servers. These cards process the voice and data signals that arrive from the CS 1000 system.

See also [Multimedia channels in the CallPilot server](#) on page 35.

Modem

The server connects to a modem to allow remote access by a support PC for installation, maintenance, and diagnostics.

Desktop client PCs

You can install desktop client messaging software on client PCs to enable mailbox users to receive phone, fax, and voicemail on their PCs. For more information, see the *Desktop Messaging and My CallPilot Installation Guide* (NN44200-305).

Any PC that has network access to the CallPilot server and has a web browser installed can be used to administer CallPilot. The CallPilot administration software is web-based.

CS 1000 Media Gateway

Introduction

The Media Gateway and Media Gateway Expansion provide the interface for analog or digital trunks, i2004 Internet phonesets, analog phonesets, and applications such as CallPilot.

Media Gateway and Media Gateway Expansion

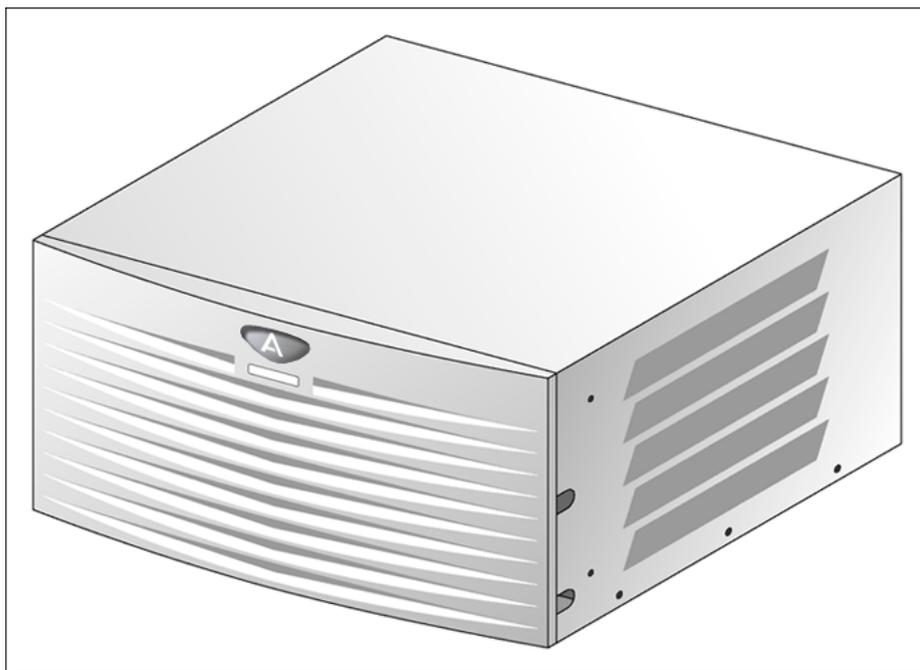
The Media Gateway and the Media Gateway Expansion provides four IPE slots. These slots support cards such as analog line cards, trunk cards, and application cards. The CallPilot 201i or 202i server is an application card that occupies two consecutive slots. The MGate Card (NTRB18CA or NTRB18DAE5) is a line card that occupies only one slot.

For a list of the cards that are supported by the CS 1000 system, see the *Communication Server 1000S or 1000E: Installation and Configuration*

! **Important:**

Media Gateway shelves in a CS 1000E do not share the same clock reference unless there is a sync cable connecting the two shelves. Media Gateway expander shelves share the same clock reference as the Media Gateway shelf that they are connected to. In a CS 1000E, all MGate cards connected to the CallPilot system must reside in the same Media Gateway/ Media Gateway Expansion shelf pair unless there is a sync cable connecting Media Gateways. For the CS 1000M and CS 1000S, the MGate cards can reside in separate shelves.

[Figure 4: Media Gateway](#) on page 25 shows a Media Gateway.



G101624

Figure 4: Media Gateway

Except for the back panel connectors, the Media Gateway Expansion is similar in external appearance to the Media Gateway.

The MGate Card (NTRB18CA or NTRB18DAE5), applicable to tower or rackmount servers only, occupies one slot in the CS 1000 system.

For information about the CS 1000 card slots in relation to the 201i or 202i server, see *CallPilot <server_model> Server Hardware Installation Guide* (NN44200-317).

Section B: Understanding call routing

In this section

[CS 1000 call routing components](#) on page 26

[Phantom DNs](#) on page 28

[CallPilot Service Directory Numbers and the SDN Table](#) on page 30

[How calls are routed](#) on page 33

[Multimedia channels in the CallPilot server](#) on page 35

[How multimedia channels are acquired by callers](#) on page 36

CS 1000 call routing components

Introduction

The CS 1000 system uses the following components to route calls:

- Automatic Call Distribution (ACD)
- Control Directory Number (CDN)

Automatic Call Distribution

Automatic Call Distribution (ACD) is a feature on the CS 1000 system that allows a number of programmed phonesets, known as ACD agents, to share equally in answering incoming calls.

In the case of CallPilot, the call-queuing capability of ACD is not used, but the call-handling capability of ACD agents is used.

How CallPilot uses ACD virtual agents

All ACD agents that service CallPilot are put into a single ACD agent queue (unless you are enabling the Contact Center Voice Services Support feature; see [How multimedia channels are acquired by callers](#) on page 36). These agents correspond to DS0 channels on the CallPilot server. Agents are programmed in overlay 11 as 2008 Digital (Aries) sets with Multimedia Messaging Allowed (MMA) class of service. These are not, however, physical phonesets. These are Terminal numbers (TNs) that are programmed to look like real digital sets to the CS 1000 system.

Control Directory Number

For CallPilot, you configure one Control Directory Number (CDN) on the CS 1000 system for each of the following services:

- a primary CDN for Voice Messaging
- a secondary CDN for Multimedia Messaging

A CDN queue is like an ACD queue. The key difference is that calls in the CDN queue are managed by CallPilot, while calls in an ACD queue are managed by the CS 1000 system.

Calls are routed to the CDN queue directly or by terminating on a phantom DN or dummy ACD queue, which is forwarded to the CDN.

How CallPilot uses CDNs

A CDN can operate in one of two modes:

- control mode
- default mode

Normally, a CDN operates in control mode. In control mode, call treatment and call routing are under the control of the CallPilot server. The CS 1000 system simply provides routing to CallPilot. The server specifies the type of treatment to be given to waiting calls. The server processes the calls on a first-come, first-served basis and determines to which DS0 channel the call is routed. DS0 channels are configured as agents of an ACD queue.

A CDN can also operate in default mode (for example, when CallPilot is offline or the AML is down). In default mode, the CS 1000 system takes over call-routing control. Incoming calls receive default treatment provided by the default ACD DN associated with the CDN.

Call queuing

Incoming calls to the CDN are queued in the order of arrival. If calls cannot be processed immediately and must wait in the queue until resources are available, the first caller in the queue is handled first.

Call routing

The CallPilot server determines which DS0 channel can provide the dialed service requested by a waiting call, and instructs the CS 1000 system to route the call to the associated ACD agent.

See also

[Phantom DNs](#) on page 28

Phantom DNs

Introduction

Instead of using phonesets or dummy ACD DNs to route calls, CallPilot can use "virtual telephones" that exist only in software and have no associated hardware. The DN associated with one of these phantom phones is called a phantom DN.

Creating a Phantom DN

To create a phantom DN, you first create a phantom loop, and then you define a TN within that loop. The system recognizes that any TN defined within that loop is a phantom TN. Each phantom TN is assigned a DN (the phantom DN). When the DN is entered in the CallPilot Service Directory Number page, it becomes the dialable number of a CallPilot service.

Phantom DNs forward to a CDN queue

Incoming calls cannot queue up in the phantom TN as they arrive. When a call arrives at a phantom DN, the system forwards it to a CDN queue before it is routed to a multimedia channel for further call handling. However, the system remembers the phantom DN to keep track of the requested service.

Services that should use phantom DNs

Avaya strongly recommends that you use either phantom DNs or dummy ACD DNs (see [Configuring ACD agents](#) on page 87) for the following services:

- all services created with Application Builder that are directly dialable by callers
- Speech Activated Messaging
- Paced Speech Messaging
- Voice Item Maintenance
- Fax Item Maintenance
- Express Voice Messaging
- Express Fax Messaging

Networking services

The following Networking services can either have a unique phantom DN configured on the CS 1000 system, or they can share the phantom DN (and SDN) of another service:

- Enterprise Networking
- AMIS Networking
- Integrated AMIS Networking

Share DNs when your supply of available DNs on the CS 1000 system is low. Create a unique DN when you need to closely monitor each service (for example, so that each service generates its own traffic data in Reporter).

 **Note:**

After you configure the SDN in CallPilot, specify with which service you are sharing the SDN.

Example

You are ready to put a new menu application into service. Phantom DN 6120 is available on the CS 1000 system. In the Service Directory Number page, you type 6120 as the SDN for this service. This is the number that callers dial to access the menu.

CallPilot Service Directory Numbers and the SDN Table

Introduction

When a call arrives at a CDN queue either directly or indirectly from a phantom DN or dummy ACD DN, the CS 1000 system gives the caller ringback treatment. While this happens, the dialed DN is looked up in the SDN Table in CallPilot to determine what service is required.

What is the SDN Table?

The SDN Table is where the CDNs, phantom DNs, or dummy ACD DNs that have been configured on the CS 1000 system for your CallPilot services are recorded. In this table, the DN (now called an SDN) is associated with a specific service. You use the CallPilot Manager Service Directory Number page to administer the SDN Table.

What the SDN Table controls

In addition to specifying which service should be activated when a number is dialed, the SDN Table also controls

- the type of channel the service acquires (voice, fax, or speech recognition)
- the number of channels allocated to the service

The SDN configuration determines the minimum number of channels guaranteed to a service for simultaneous use and the maximum number of channels that you can use at one time.

- the session behavior for certain services, such as those created with Application Builder (including the maximum session length and a number of fax options)

Types of SDNs

There are two types of SDNs--inbound SDNs and outbound SDNs.

Inbound SDNs require DNs on the CS 1000 system

Services that callers dial need inbound SDNs. An inbound SDN corresponds to either a CDN, a phantom DN, or a dummy ACD DN on the CS 1000 system, since callers must be able to dial in to the CS 1000 system with a unique number.

Outbound SDNs do not require DNs on the CS 1000 system

Callers do not dial outbound SDNs. The system uses outbound SDNs to place outbound calls. Because outbound SDNs do not accept incoming calls, a corresponding CDN, phantom DN, or dummy ACD DN is not necessary on the CS 1000 system.

The following services use outbound SDNs:

- outcalling services (Remote Notification, Delivery to Telephone, Delivery to Fax)
- networking services (AMIS Networking and Enterprise Networking)

How calls are routed

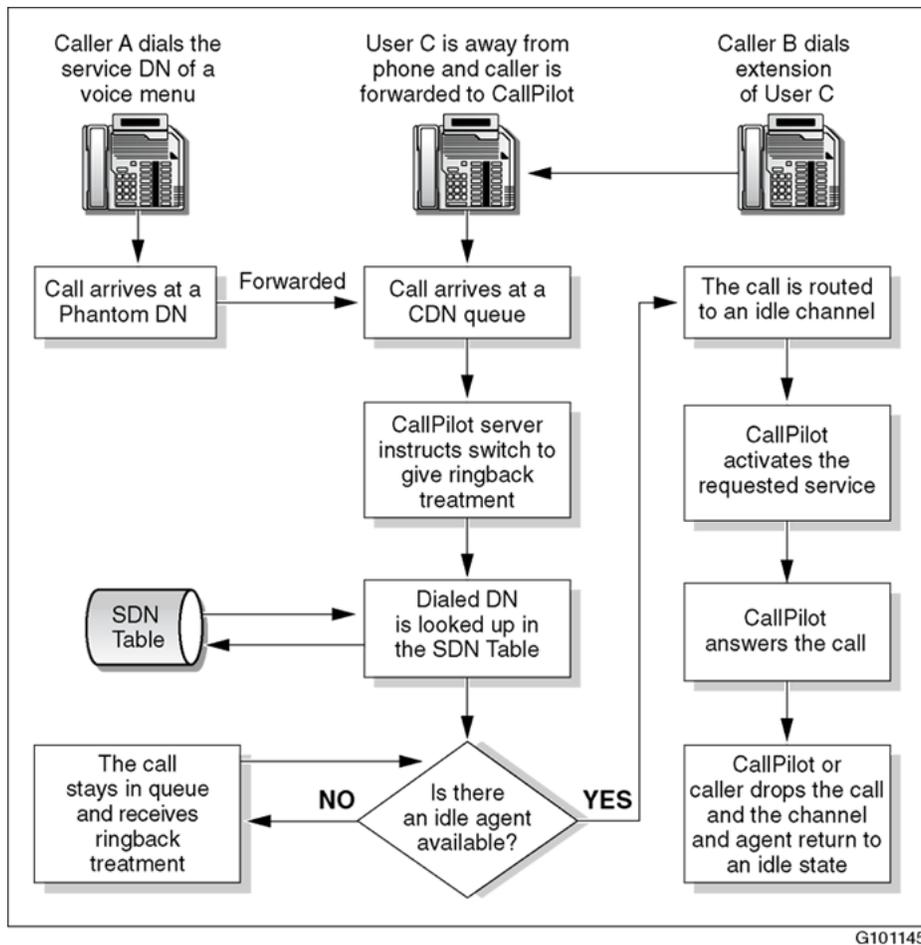


Figure 5: Call flow example

*** Note:**

The example above uses a phantom DN. The same call flow occurs when a caller dials a dummy ACD DN.

Example of phantom DN or dummy ACD DN usage

Two CDN queues have been configured:

- Voice Messaging (6030)
- Multimedia Messaging (6050)

Two phantom DNs have been configured (the same scenario applies if these are set up as dummy ACD DNs):

- 6090 is the DN for a menu service (without fax items)
- 6095 is the DN for Fax Item Maintenance

In [Figure 6: No available channels, calls queued](#) on page 34, when the calls come in to the CS 1000 system, there are no available channels, and the calls are queued as a result.

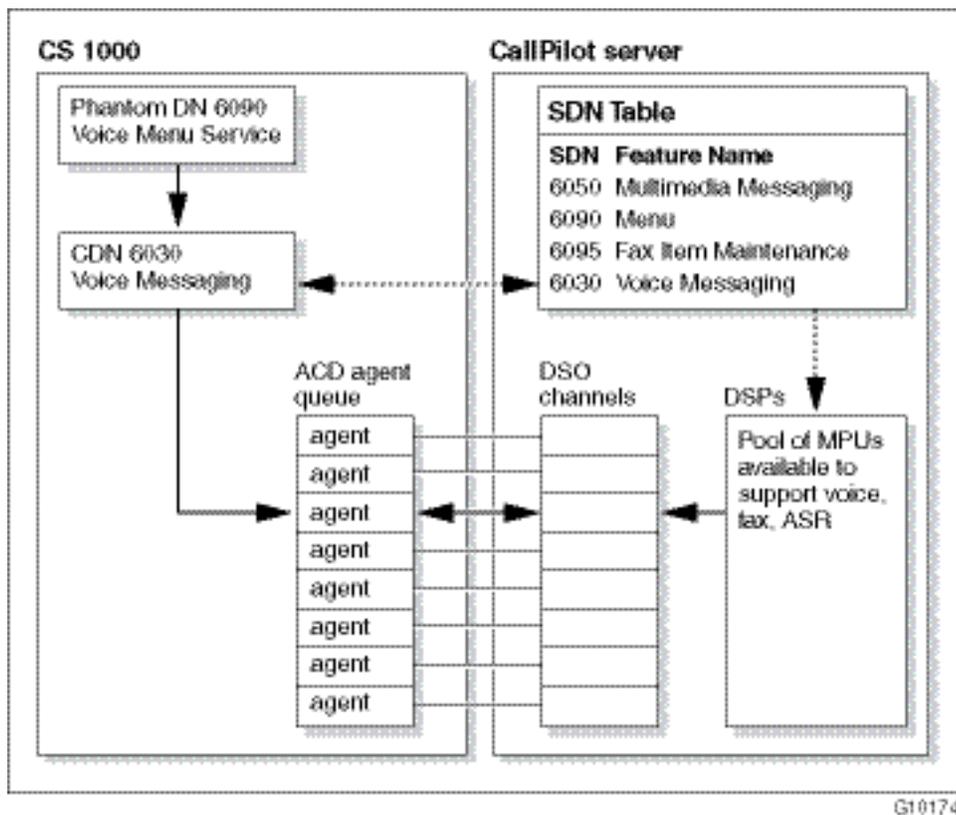


Figure 6: No available channels, calls queued

What happens when users dial the service DNs

1. A caller dials 6090 to access a menu service. This phantom DN forwards to CDN 6030 because the menu contains no fax or speech recognition capability.
2. Another caller dials 6095 to access the Fax Item Maintenance service. The call is forwarded to CDN 6050.
3. CallPilot looks up the DNs in the SDN Table on the server to check which service is being requested, the media type required, and the channel allocations for each service.
4. Call 1, to the menu service that contains only voice functions (no fax items), is routed to an ACD agent that is available to handle voice.
5. Call 2, to the Fax Item Maintenance service, is routed to an ACD agent that is available to handle fax.

Multimedia channels in the CallPilot server

Multimedia Processing Units

In addition to the CPU processing power required by CallPilot, calls that are received by CallPilot require DSP processing power to support the voice, fax, and speech recognition features. DSP processing power is provided by Multimedia Processing Units (MPUs) in the CallPilot server. MPUs are provided by the following CallPilot hardware:

- MPB boards (MPB16-4 for the 1002rp server only, or MPB96)
- MPC-8 cards (if MPB16-4 boards are used)

Types of multimedia channels

Certain types of media require more channel resources to process them. As a result, three types of multimedia channels handle the various types of CallPilot services. Each type of channel terminates on a different number of MPUs, based on how much processing power is required. For example, integrated fax and voice data takes twice as much processing power as voice-only media. A fax channel, therefore, terminates on two MPUs.

Table 3: Number of MPUs per Channel Type

Channel type	Number of MPUs	Description
Voice	1	One voice channel requires one MPU.
Fax	2	Fax requires twice as much processing power as voice-only media, and, therefore, requires two MPUs for one fax channel.
ASR (automated speech recognition)	4	Speech recognition requires four times as much processing power as voice-only media, and, therefore, requires four MPUs for one speech recognition channel.

How multimedia channels are acquired by callers

Introduction

The system uses the information gathered from the SDN configuration to check the ACD agent queue to determine if an idle multimedia channel of the type required by the service is available.

IF	THEN
an idle channel (of the required media type) is available	the system passes the call to CallPilot.
idle channels that meet the requirements defined in the SDN Table are not available	the call remains in the CDN queue and the system applies a delay treatment. The server specifies a default delay treatment of ringback. This means that while a call waits in a queue, the caller hears the phone ringing.

What happens when the call is answered

When a multimedia channel of the appropriate type becomes idle, the call arrives at the multimedia channel and is passed to CallPilot.

Because the SDN Table has already been checked, the requested service is known and is activated. The service also answers the call.

Based on which service is activated, one of the following results happens:

- The appropriate prompt is played.
- CallPilot receives a fax.
- CallPilot records a message.

What happens when the call is dropped

When CallPilot or the caller drops the call (hangs up), the multimedia channel returns to an idle state, ready to be acquired by another call.

What is next?

IF your server is a	THEN
tower or rackmount server (600r, 703t, 1002rp, 1005r, or 1006r)	continue with Section B: Connecting the CallPilot server to the switch on page 50.
201i or 202i server	continue with Configuring the Avaya Communication Server 1000 system on page 71.

Chapter 3: Connecting the Avaya CallPilot® server to the Avaya Communication Server 1000 system

In this chapter

[Section A: Installing the MGate card](#) on page 39

[About the MGate card \(NTRB18CA or NTRB18DAE5\)](#) on page 40

[Installing the MGate card \(NTRB18CA or NTRB18DAE5\)](#) on page 45

[Replacing an MGate card \(NTRB18CA or NTRB18DAE5\)](#) on page 48

[Section B: Connecting the CallPilot server to the switch](#) on page 50

[About the MGate cables](#) on page 51

[Connecting MPB16-4 boards to MGate cards \(NTRB18CA or NTRB18DAE5\)](#) on page 55

[Connecting the MPB96 boards to MGate cards \(NTRB18CA or NTRB18DAE5\)](#) on page 61

Section A: Installing the MGate card

In this section

[About the MGate card \(NTRB18CA or NTRB18DAE5\)](#) on page 40

[Installing the MGate card \(NTRB18CA or NTRB18DAE5\)](#) on page 45

[Replacing an MGate card \(NTRB18CA or NTRB18DAE5\)](#) on page 48

About the MGate card (NTRB18CA or NTRB18DAE5)

Introduction

The MGate card (NTRB18CA or NTRB18DAE5) is the line interface card in the CS 1000 system that supports the call channels for Avaya CallPilot. When connecting the MGate card to the CallPilot server, there are different cabling scenarios depending on the card combinations for your site. For more information see [Table 10: MGate cabling scenarios](#) on page 51

 **Note:**

The MGate card is hot-swappable. Therefore, you do not need to power down the CS 1000 system before installing or removing an MGate card.

 **Important:**

An MGate card is not used with the 201i or 202i server. For the 201i or 202i server, the connection to the CS 1000 system is established in the Media Gateway or Media Gateway Expansion when the server is installed. For more information, see the CallPilot <server_model> Server Hardware Installation Guide.

 **Important:**

Media Gateway shelves in a CS 1000E do not share the same clock reference unless they are connected by a sync cable. Media Gateway expander shelves share the same clock reference as the Media Gateway shelf that they are connected to. In a CS 1000E, all MGate cards connected to the CallPilot system must reside in the same Media Gateway/Media Gateway Expansion shelf pair unless the Media Gateways are connected by a sync cable. For the CS 1000M and CS 1000S, the MGate cards can reside in separate shelves.

The NTRB18DAE5 MGate card is backward compatible to the NTRB18CA MGate card and can be connected to any MPB board. The newer NTRB18DAE5 MGate card can be connected to the CallPilot server using a standard "off the shelf" cable up to 600 metres (1968 ft) in length. This enables you to install the CallPilot server in a location that is remote from the CS1000.

The following table compares the two MGate card versions.

Table 4: MGate card version comparison

MGate version	Description
NTRB18CA	Is not equipped with a faceplate connector Can NOT be connected to an NTRH40CAE5 MPB96 board in the CallPilot server

NTRB18DAE5	Is equipped with an RJ-45 faceplate connector Can be connected to any MPB card in the CallPilot server
------------	---

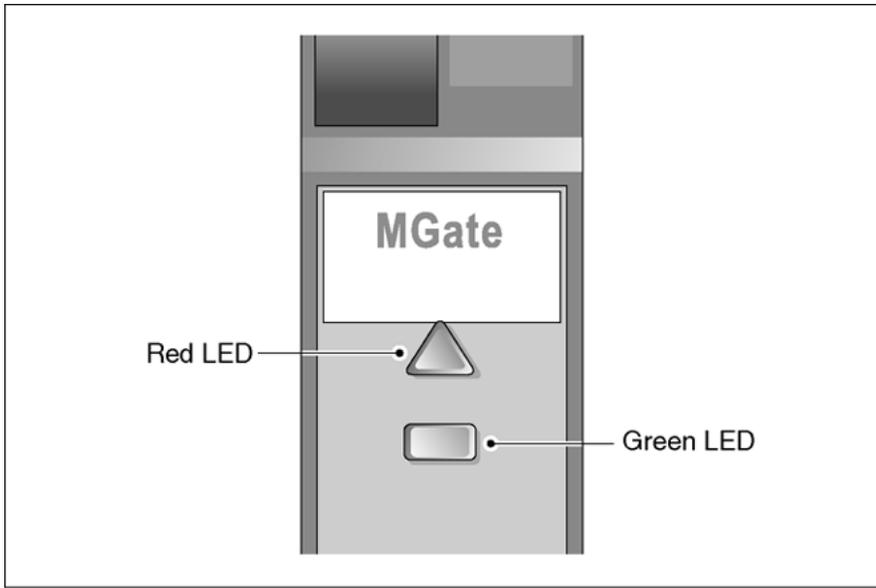
Number of channels supported

Each MGate card (NTRB18CA or NTRB18DAE5) supports 32 channels. These 32 channels can be any combination of voice, fax, and automated speech recognition channels. For example, you can have 16 voice, 8 fax, and 8 automated speech recognition channels supported by a single MGate card.

On the CallPilot server side, you require additional DSP MPUs to support fax or automated speech recognition channels, but this does not affect the number of channels supported by the MGate card.

LED indicators

The MGate card (NTRB18CA or NTRB18DAE5) has red and green LED indicators near the top of the faceplate. For an explanation of the green and yellow LED indicators on the RJ-45 connector on the NTRB18DAE5, see [NTRB18DAE5 MGate Link LED indications](#) on page 68.



G101794

Figure 7: MGate LED indicators

The combined state of the red and green LEDs provides important indicators of the MGate card's status.

Table 5: MGate card status

Red LED	Green LED	Description
OFF	ON	The MGate card is enabled in the CS 1000 system software, and the MGate card is operational.
OFF	OFF	The MGate card is not receiving power, or the MGate card is faulty.
ON	ON	The MGate card is disabled in the CS 1000 system software, but the MGate card is operational.
ON	OFF	The MGate card is disabled in the CS 1000 system software, and the MGate card is faulty.
blinking	blinking	The MGate card is executing self-test diagnostics.

Impact of a faulty MGate card (NTRB18CA or NTRB18DAE5)

The CS 1000 system may or may not recognize when an MGate card is faulty. If the CS 1000 system does recognize the problem, then it automatically disables the MGate card and informs CallPilot that the MGate card is faulty.

If the CS 1000 system does not recognize that the MGate card is faulty, it does not automatically disable it. In this situation, you must use overlay 32 to manually disable the MGate card slot.

The DS0 channels associated with the disabled MGate card are taken out of service by CallPilot and assigned a Remote Off Duty status. If there are multiple MGate cards, and if the faulty MGate card is not the first MGate associated with the first STI link, then CallPilot will continue to use the DS0 channels associated with the functioning MGate cards.

Required components

There are two MPB96 board versions; the NTRH40AA/NTRH40AAE5 which is identified by a single DB-44 faceplate connector, and the NTRH40CAE5 which is identified by three RJ-45 faceplate connectors. The required components depend on the version of your MPB96 boards

Table 6: For CallPilot servers using NTRH40AA MPB96 boards

Component	Part Number	Description
MGate card	NTRB18CA or NTRB18CAE5 or NTRB18DAE5	Installed in the Media Gateway or Media Gateway Expansion. The MGate card is available in two versions listed in the part number column. For a comparison of the two cards, see Table 4: MGate card version comparison on page 40.
DS30X Cable	NTRH2014	Connects the MPB96 boards in the CallPilot server to the MGate cards (NTRB18CA or NTRB18DAE5) in the Media Gateway or Media Gateway Expansion.

If you are connecting to a Communication Server 1000S or to a Communication Server 1000E, you may connect the DS30 cable to the RJ-45 faceplate connector or to the backplane connector of the NTRB18DAE5 MGate card. If you are connecting to a Communication Server 1000M, you must connect to the backplane connector of the NTRB18DAE5 MGate card. The following table describes the required components for each type of connection.

Table 7: For CallPilot servers using NTRH40CAE5 MPB96 boards

Component	Part Number	Description
MGate card	NTRB18DAE5 only	Installed in the Media Gateway or Media Gateway Expansion. The MGate card is available in two versions. To identify your MGate card, see Table 4: MGate card version comparison on page 40.

Component	Part Number	Description
Connecting cable	N/A	The cable is a customer supplied CAT5e (or better) unshielded twisted pair (UTP) Ethernet type cable. For further information about the connecting cable, see Cables supported by the NTRH40CAE5 MPB96 board on page 54.
RJ-45 to 50 pin telephony MDF connector adapter (optional)	N0193176	Connects the customer supplied cable to the backplane connector of the NTRB18DAE5 MGate card (CS 1000M only)
Shielded twisted pair cable	NTDU0609	Used when connecting to CS 1000E or CS 1000S MGate faceplate RJ-45 only. Connects the customer supplied cable to the RJ-45 connector on the MGate card. Not required if you are connecting to the MGate backplane connector Decreases EMI to acceptable levels
Shielded twisted pair cable	NTDK8305	Used when connecting to an MGate in an Option 11C cabinet only. Connects the customer supplied cable to the RJ-45 connector on the MGate card. Not required if you are connecting to the MGate backplane connector Decreases EMI to acceptable levels

 **Caution:**

Do not connect the CAT5e cable to the RJ-45 connector on the MGate card in a CS 1000M. Connecting the CAT5e cable to the RJ-45 connector on the MGate card results in unacceptable levels of electromagnetic interference (EMI).

Table 8: For CallPilot servers using MPB16 boards

Component	Part Number	Description
MGate card	NTRB18CA or NTRB18DAE5	Installed in the Media Gateway or Media Gateway Expansion.
		 Note: The MGate card is available in two versions listed in the previous column. For a comparison of the two cards, see Table 4: MGate card version comparison on page 40
DS30X cable	NTRH2012 NTRH2013	Connects the MPB16-4 boards in the CallPilot server to the MGate

- Single cable
 - Dual cable
- cards in the Media Gateway or Media Gateway Expansion.
-

Installing the MGate card (NTRB18CA or NTRB18DAE5)

Introduction

This section describes how to

- set the MGate card's DIP switches (NTRB18CA only)
- install the MGate card in the Media Gateway or Media Gateway Expansion
- replace the MGate card

Before you begin

To minimize network blocking, see the CS 1000 Planning and Engineering guide for segmenting and traffic rules. Determine which slot you will use to house the MGate card. You can install MGate cards on all IPE slots in the Media Gateway or Media Gateway Expansion.

 **Important:**

Media Gateway shelves in a CS 1000E do not share the same clock reference unless they are connected together by a sync cable. Media Gateway expander shelves share the same clock reference as the Media Gateway shelf that they are connected to. In a CS 1000E, all MGate cards connected to the CallPilot system must reside in the same Media Gateway/ Media Gateway Expansion shelf pair unless the Media Gateways are connected together by a sync cable. For the CS 1000M and CS 1000S, the MGate cards can reside in separate shelves.

For more information about card slots, see the Communication Server 1000S: Installation and Configuration.

MGate Card (NTRB18CA) DIP switches

[Figure 8: MGate DIP switches](#) on page 46 shows an MGate card with the location of the DIP switches.

*** Note:**

The NTRB18DAE5 MGate card does not have DIP switches. If you have an NTRB18DAE5 MGate card, go to [To install the MGate card](#) on page 47.

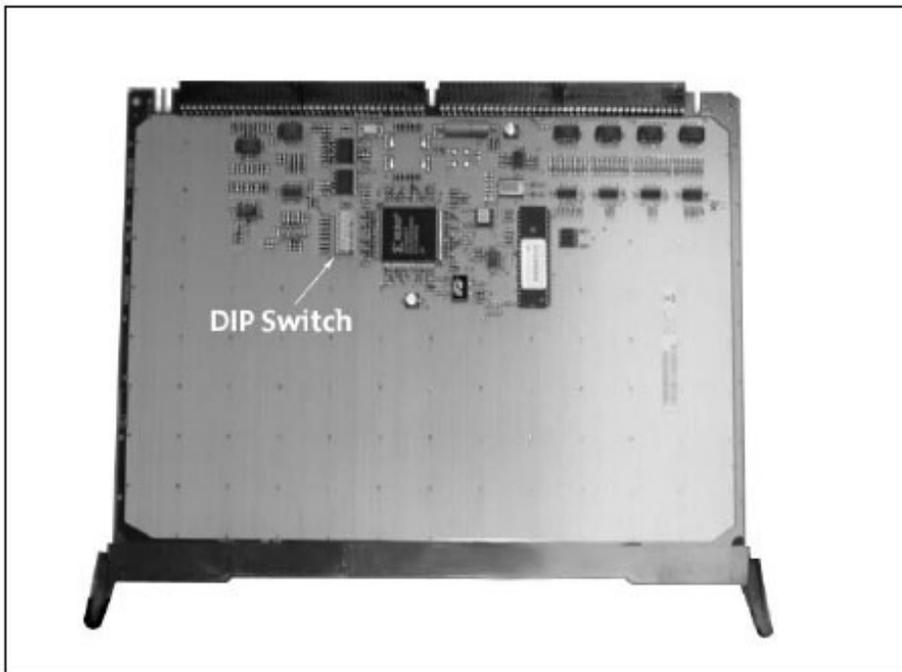


Figure 8: MGate DIP switches

To set the DIP switches for the MGate card (NTRB18CA only)

1. Remove the MGate card from its protective sleeve.
2. Set the DIP switches on the MGate card as shown in [Table 9: MGate DIP switch settings](#) on page 46. These DIP switch settings are used for all MGate cards and all system configurations.

Table 9: MGate DIP switch settings

	1	2	3	4	5	6	7	8
ON	X	X	X				X	
OFF				X	X	X		X

To install the MGate card

1. Remove the Media Gateway or Media Gateway Expansion cover.
2. Ensure that the slot in which you are installing the MGate does not already have a cable connected.
3. Press and pull the top and bottom latches on the MGate card outward to open the latches for installation of the card.

A hook on the bottom of the latch must clear a small pin to open. see [Figure 9: Media Gateway slot latch](#) on page 47.

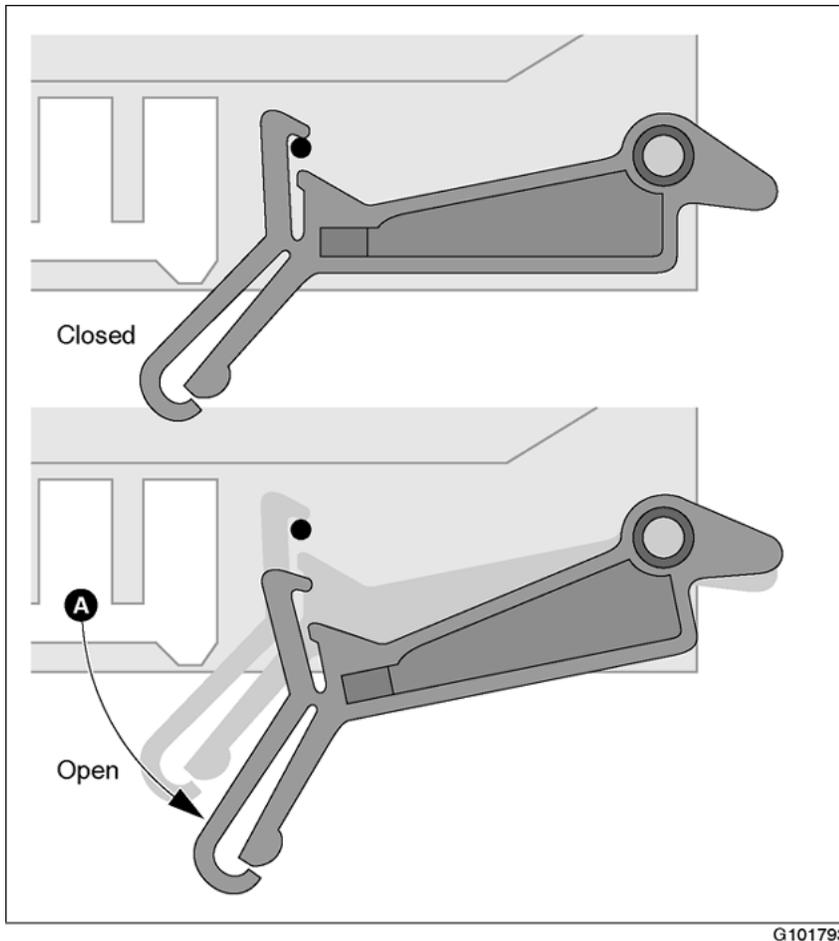


Figure 9: Media Gateway slot latch

4. Slide the MGate card into an unoccupied slot.

When correctly inserted, the top of the MGate card is on the left. See the following diagram.

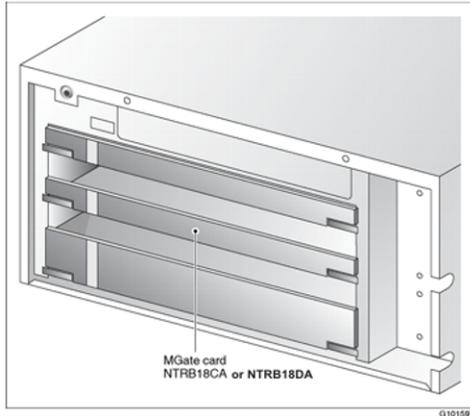


Figure 10: MGate cards in slots

5. Press the lock latches to close them.

This locks the MGate card into position against the backplane.

6. View the status of the LED indicators to ensure that the card is software-enabled (red LED is OFF) the card is operational (green LED is ON)

For more information about the LEDs, see [LED indicators](#) on page 41.

7. Replace the inside front cover plate and front bezel.

! **Important:**

Ensure that the tabs on the bottom and right side of the inside front cover plate are positioned inside the Media Gateway or Media Gateway Expansion.

What is next?

Continue with [Section B: Connecting the CallPilot server to the switch](#) on page 50.

Replacing an MGate card (NTRB18CA or NTRB18DAE5)

Introduction

If the MGate card becomes faulty, follow this procedure to replace it.

There are two versions of the MGate card available: The NTRB18CA, and the NTRB18DAE5. You can replace an NTRB18CA with an NTRB18DAE5. It is important to know which type of

MPB is in your CallPilot server. The following table identifies which MGate card versions can be used in your CS 1000.

For this MPB card	You can install these MGate card versions
NTRH40AA MPB96	NTRB18CA or NTRB18DAE5 (Both versions can reside together on your Communication Server 1000)
NTRH40CAE5 MPB96	NTRB18DAE5 only
MPB16-4	NTRB18CA or NTRB18DAE5 (Both versions can reside together on your Communication Server 1000)

To replace an MGate card

Note:

You do not need to power down the switch for this procedure as the MGate card is hot-swappable.

1. Courtesy stop the DS0 channels from the CallPilot administrative PC to stop all call processing gracefully.

To do this, use the Channel Monitor or the Maintenance page in CallPilot Manager, as described in the CallPilot Server Maintenance and Diagnostics guide for your server.

Note:

If your system has multiple MGate cards, you can choose to courtesy stop only the DS0 channels that belong to the MGate card that is being replaced.

2. Remove the switch's front cover to expose the shelf slots.
3. If there is a cable connected to the faceplate of the faulty MGate card, disconnect the cable from the card.
4. Open the latches to unlock the faulty MGate card.
5. Remove the faulty MGate card from the switch.
6. Press the replacement MGate into the same slot that the faulty MGate card occupied.

Note:

Note: If you place the MGate card in a new slot, then you must do the following:

- a. Reprogram the switch to account for the new slot number.
 - b. Move the cable to the new slot.
 - c. Reconfigure the software from the CallPilot administrative client PC.
7. Press the latches on the top and bottom of the MGate card to close them.
Result: This locks the card into position against the backplane.
 8. Reinstall the DS30/CAT5 cable (if applicable).
 9. View the status of the LED indicators to ensure that the card is software-enabled (red LED is off), and the card is operational (green LED is on). If you have an NTRB18DAE5 connected to an NTRH40CAE5 MPB96, check the RJ-45 LEDs to ensure that the link is enabled (green LED on and yellow LED off).
 10. Re-enable the DS0 channels that were disabled before the card was removed.
To do this, use the Channel Monitor or the Maintenance page in CallPilot Manager, as described in the CallPilot Server Maintenance and Diagnostics guide for your server.

Section B: Connecting the CallPilot server to the switch

In this section

[About the MGate cables](#) on page 51

[Connecting MPB16-4 boards to MGate cards \(NTRB18CA or NTRB18DAE5\)](#) on page 55

[Connecting the MPB96 boards to MGate cards \(NTRB18CA or NTRB18DAE5\)](#) on page 61

About the MGate cables

Introduction

Depending on your hardware types or versions, there are different scenarios for cabling your MGate cards to the CallPilot server. The following table describes the scenarios, and directs you to the applicable section for further information.

- The NTRH40AA MPB96 board can be identified by a single DB-44 connector on its faceplate.
- The NTRH40CAE5 MPB96 board can be identified by three RJ-45 connectors on its faceplate.
- The MPB16-4 board can be identified by a DB-25 connector on the its faceplate.

Table 10: MGate cabling scenarios

Scenario	For this MPB card	Supported MGates	Supported cables	See this section for more information
1	MPB16-4	NTRB18CA or NTRB18DAE5	DS30X cable: single cable NTRH2012 or Dual cable NTRH2013	DS30X cables supported by MPB16-4 boards on page 52
2	MPB96 (NTRH40AA)	NTRB18CA or NTRB18DAE5	DS30X cable NTRH2014	DS30X cable supported by the NTRH40AA MPB96 board on page 53
3	MPB96 (NTRH40CAE5)	NTRB18DAE5	DS30 cable: Customer supposed (UTP CAT5e or better)	Cables supported by the NTRH40CAE5 MPB96 board on page 54
		NTDU0609	Shielded twisted pair cable for EMI prevention (connects the	

Scenario	For this MPB card	Supported MGates	Supported cables	See this section for more information
			customer supplied CAT5 cable to the MGate faceplate on CS 1000E and CS 1000S)	
		NTDK8305	Shielded twisted pair cable for EMI prevention (connects customer supplied CAT5 cable to the MGate faceplate on Option 11C cabinet)	



Note:

For scenarios 1 and 2, both versions of MGate cards can be connected to the same MPB card. For scenario 3, use a Merteck N0193176 adapter if you are connecting to the MGate backplane connector (CS 1000M only).



Caution:

Do not connect the CAT5 cable directly to the Mgate faceplate in a CS 1000M as this results in unacceptable electromagnetic interference (EMI). Use a Merteck N0193176 adapter to connect the CAT5 cable to the backplane connector at the rear of the UEM. For the connection procedure, see the appropriate heading under [High capacity configuration](#) on page 66

DS30X cables supported by MPB16-4 boards

The DS30X cable that establishes the connection between the MPB16-4 boards and the MGate cards is 10 m (30 ft) long. Therefore, the CallPilot server must be placed within 10 m (30 ft) of the Media Gateway or Media Gateway Expansion.

the server is equipped with	the DS30X cable is an
one MPB16-4board	NTRH2012 cable. This is a single DS30X cable that connects one MPB16-4 board to one MGate card.
more than one MPB16-4 board	NTRH2013 cable.

the server is equipped with	the DS30X cable is an
	This is a dual DS30X cable that connects the first of two MPB16-4 boards to two MGate cards. The connectors on the NTRH2013 dual DS30X cable are labeled DS30X-1 and DS30X-2.



Note:

The NTRH2012 and NTRH2013 cables contain ferrites that control EMC emission levels. Do not remove them.

To connect your MGate card to the MPB16-4 on the CallPilot server, see [Connecting MPB16-4 boards to MGate cards \(NTRB18CA or NTRB18DAE5\)](#) on page 55

DS30X cable supported by the NTRH40AA MPB96 board

The NTRH2014 cable is a triple DS30X cable that connects the MPB96 board to up to three MGate cards. The cable is 20 m (60 ft) long, allowing you to install the CallPilot server in a different room from the Media Gateway or Media Gateway Expansion.

One end of the cable has a 44-pin connector that connects to the MPB96 board's faceplate. If the server is equipped with more than one MPB96 board, the cable connects to the first board (the board in the lowest numbered slot of the server).

The other end of the cable has three 50-pin connectors that connect to MGate cards. The MGate connectors are labeled DS30X-1, DS30X-2, and DS30X-3.

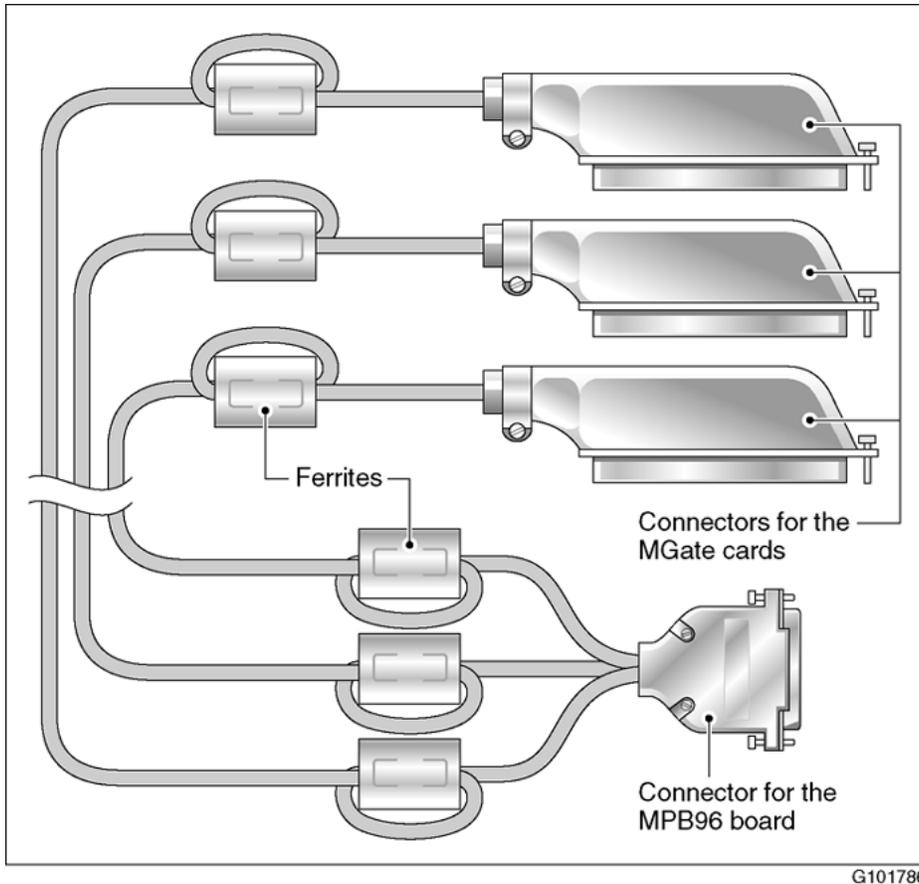


Figure 11: Connectors between MGate and NTRH40AA MPB96

*** Note:**

The ferrites on this cable control EMC emission levels. Do not remove them.

For more information about connecting your MGate card to an NTRH40AA MPB96 on the CallPilot server, see [MGate cabling to the NTRB18DAE5 MPB96 card \(703t, 1002rp, 600r, 1005r\)](#) on page 62.

Cables supported by the NTRH40CAE5 MPB96 board

The connecting cables are standard RJ-45 connectorized Ethernet cables made with CAT5e (or better) Unshielded Twisted Pair (UTP) cable with standard Ethernet pinouts (no crossover). The cable can be up to 600 m (1968 ft.) long, allowing you to install the CallPilot server in a location that is remote from the Media Gateway or Media Gateway Expansion.

The cable connects to the RJ-45 connector on the faceplate of the NTRB18DAE5 MGate card and to one of three RJ-45 connectors on the NTRH40CAE5 MPB96 board.

The cable cannot be connected to the RJ-45 connector on an MGate card that is installed in a CS 1000M. When connecting to an MGate in a CS 1000M, a Merteck N0193176 RJ-45 to 50 pin Amphenol adaptor is required. The Merteck N0193176 adaptor allows you to connect the cable to the backplane connector of the MGate card in the CS 1000M.

For more information about connecting your MGate card to an NTRH40CAE5 MPB96 on the CallPilot server, see [MGate cabling to the NTRH40CAE5 MPB96 card \(600r, 1005r, and 1006r\)](#) on page 65.

Connecting MPB16-4 boards to MGate cards (NTRB18CA or NTRB18DAE5)

Introduction

This section describes the MPB16-4 board and MGate card connection scenarios that your CallPilot server supports. You must use the appropriate DS30X cable for the connection scenario—either the NTRH2012 or the NTRH2013 cable.



Note:

For a description of the MPB16-4 board, see the CallPilot Server Maintenance and Diagnostics guide for your server.

Cabling diagrams

The following table lists the supported configurations and the page number that illustrates the configuration.

Table 11: Cabling configurations

Number of channels	Number of MPB16-4 boards	Number of MGate cards	See
32 or less	1	1	
32 or less	2	1	
48 or less	1	2	
48 or less	2	2	

Identifying the location of MPB 1 and MPB 2

In the cabling diagrams, the terms MPB16-4 #1 and MPB16-4 #2 are used to identify the two MPB16-4 boards. The table below indicates the location of these boards.

Table 12: MPB16-4 slot locations

MPB Number	1002rp server
MPB16-4 #1	slot 11
MPB16-4 #2	slot 12

 **Note:**

On the 1002rp servers, MPB16-4 #1 is the MPB16-4 board closest to the SBC card. For more information on slot assignments, see the slot assignment tables in the CallPilot Server Hardware Installation guide for your server.

Identifying the location of MGate 1, 2, and 3

In the cabling diagrams, the terms MGate #1, MGate #2, and MGate #3 identify the MGate cards. MGate #1 is in the lowest-numbered slot in the Media Gateway or Media Gateway Expansion. MGate #2 and MGate #3 are in the next available higher slots.

One MPB16-4 board and one MGate card (32 channels or less)

Use the single cable (NTRH2012) to connect the MPB16-4 board to the MGate card. See [Figure 12: MGate cabling for the 1002rp server](#) on page 57.

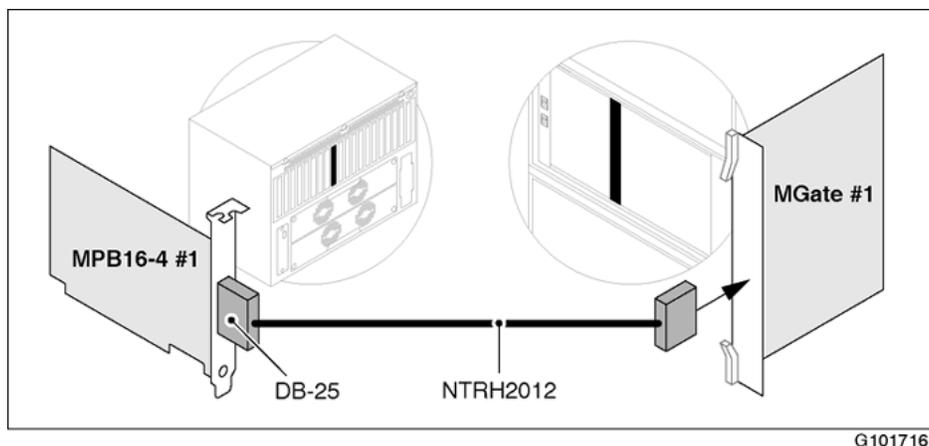


Figure 12: MGate cabling for the 1002rp server

Two MPB16-4 boards and one MGate card (32 channels or less)

Use the DS30X single cable (NTRH2012) to connect the MPB16-4 #1 to the MGate card. See [Figure 13: MGate cabling for the 1002rp server](#) on page 57 and [Figure 14: MGate cabling for the 1002rp server](#) on page 58.

Note:

The MPB number is identified during system startup. Therefore, you must connect the DS30X cable to the MPB assigned the lower bus number by the software.

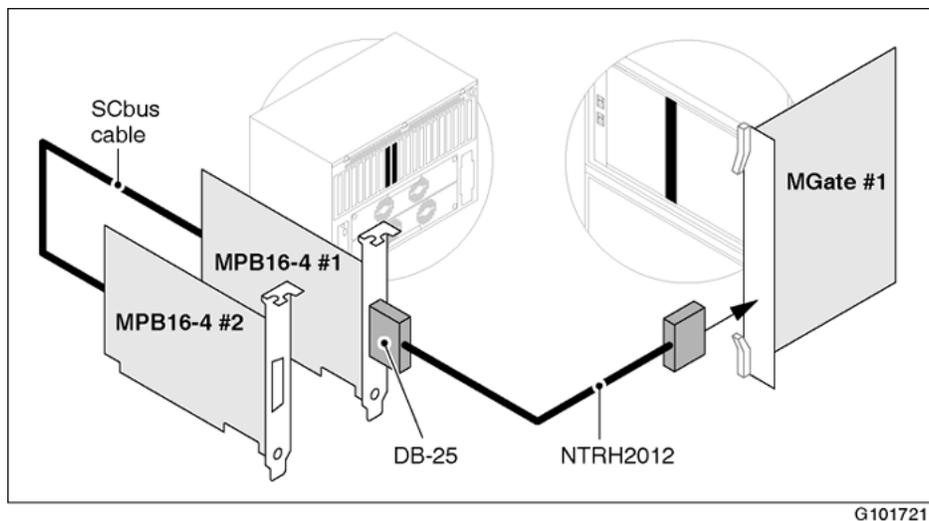


Figure 13: MGate cabling for the 1002rp server

One MPB16-4 board and two MGate cards (48 channels or less)

Use the NTRH2013 cable, as shown in the diagrams that follow. Ensure that

- the connector labeled DS30X-1 is connected to MGate #1
- the connector labeled DS30X-2 is connected to MGate #2

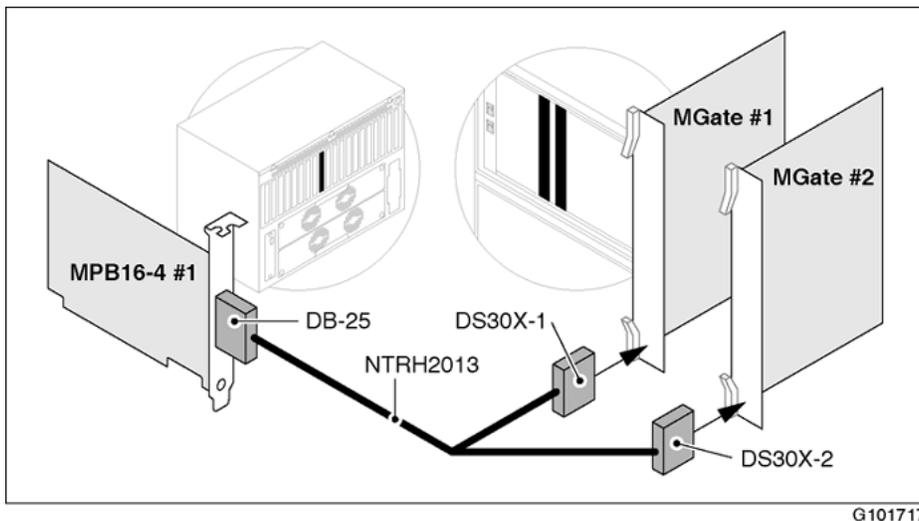


Figure 14: MGate cabling for the 1002rp server

Two MPB16-4 boards and two MGate cards (48 channels or less)

Use the NTRH2013 cable, as shown below. Ensure that

- the connector labeled DS30X-1 is connected to MGate #1
- the connector labeled DS30X-2 is connected to MGate #2

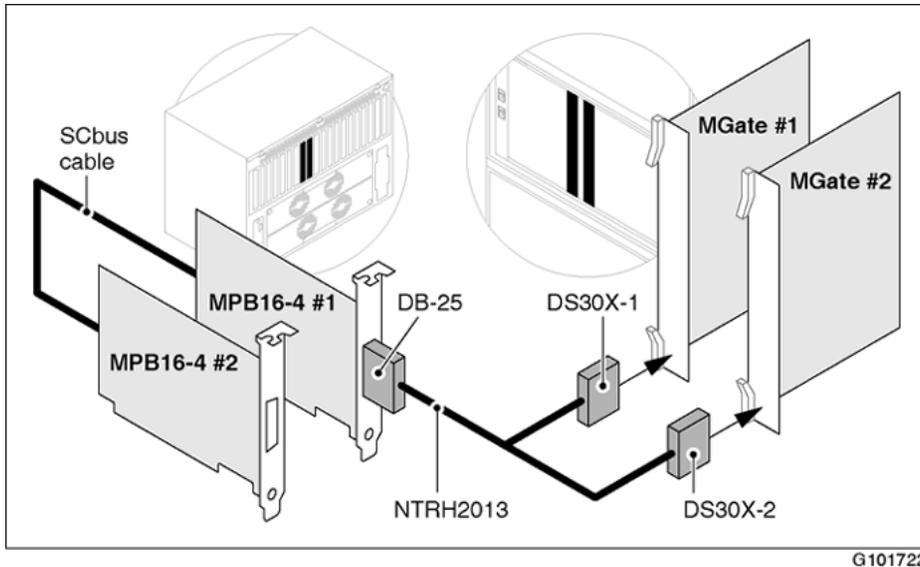


Figure 15: MGate cabling for the 1002rp server

To connect the DS30X cable

Before you begin, review the supported cabling configurations illustrated in [Table 11: Cabling configurations](#) on page 55.

1. On the side of the Media Gateway or Media Gateway Expansion, locate the connector associated with the slot occupied by the MGate card.
2. Attach the DS30X connector on the NTRH2012 or NTRH2013 cable to the slot connector as shown in the previous diagrams.
 - a. Loosen the connector's Velcro fastening strap.
 - b. Connect the amphenol connector on the MGate cable to the connector on the back of the Media Gateway or Media Gateway Expansion.
 - c. Secure the connection by tightening the connector's retaining screw and Velcro fastening strap.

The following diagram shows how to secure the MGate cable connection.

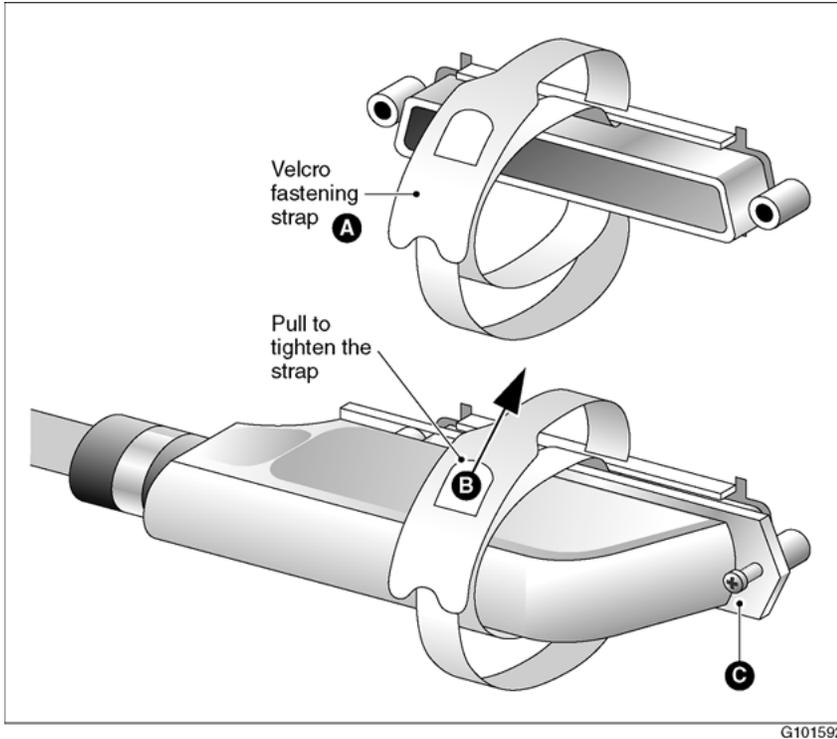


Figure 16: DS30X cable connection

3. Connect the other end of the MGate cable to the MPB16-4 board's connector on the bottom of the CallPilot server.

What is next?

Continue with [Configuring the Avaya Communication Server 1000 system](#) on page 71.

Connecting the MPB96 boards to MGate cards (NTRB18CA or NTRB18DAE5)

Introduction

The CallPilot server ships from the factory with one or more MPB96 boards already installed. Because the MPB96 board is already installed in the server, you only need to connect it to the MGate card in the CS 1000 system.

- If you have an NTRH40AA MPB96 board, use an NTRH2014 DS30X cable to connect to the NTRB18CA or NTRB18DAE5 MGate card. The NTRH40AA MPB96 board can be identified by a single DB-44 connector on the faceplate.
- If you have an NTRH40CAE5 MPB96 board, use a customer supplied CAT5e DS30 cable to connect to the NTRB18DAE5 MGate card. The NTRB18CA MPB96 board can be identified by three RJ-45 connectors on the faceplate.
- The NTRH40CAE5 MPB96 cannot be installed in a 1002rp server.
- The NTRH40CAE5 MPB96 only works with an NTRB18DAE5 or later version MGate card.

You connect the MPB96 board to up to three MGate cards depending on the number of DS0 channels. If fewer than three MGate cards are present, you can leave the unused parts of the NTRH2014 cable unconnected.

 **Note:**

For a description of the MPB96 board, see the CallPilot Server Maintenance and Diagnostics guide for your server.

MGate cabling to the NTRB18DAE5 MPB96 card (703t, 1002rp, 600r, 1005r)

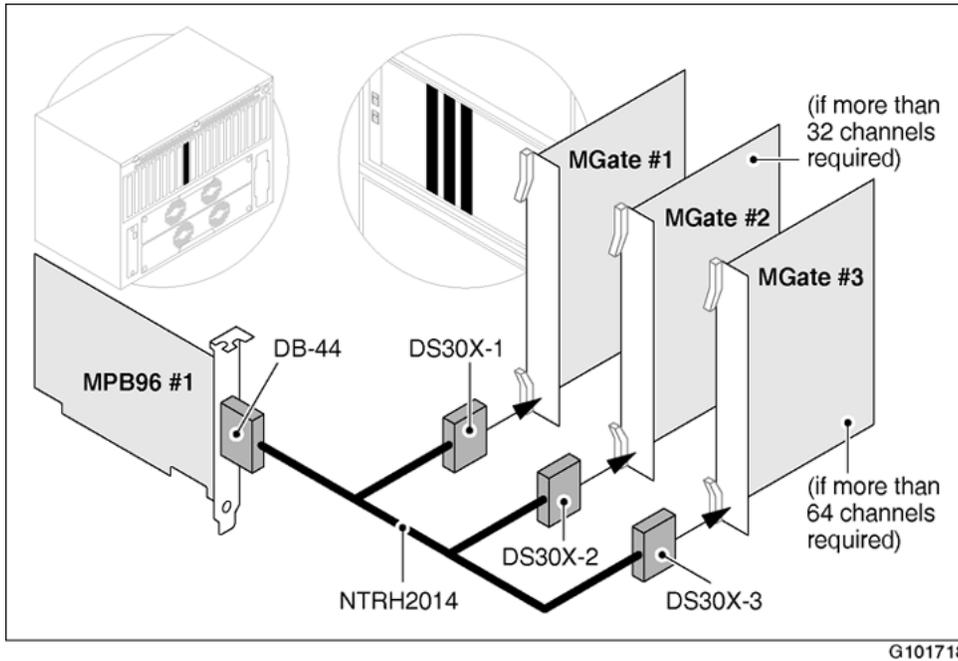
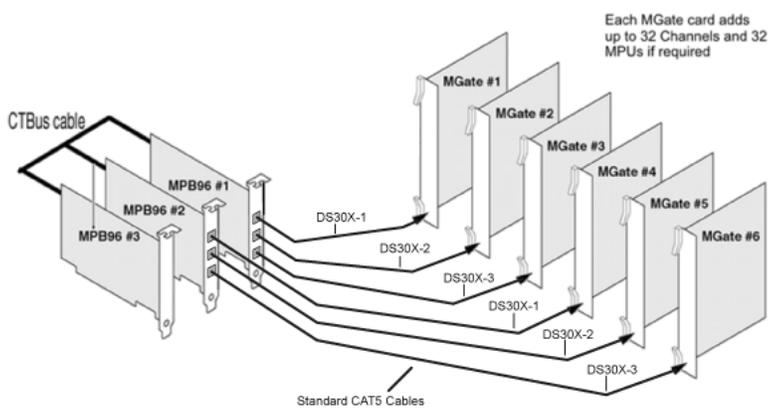


Figure 17: One MPB96 board and three MGate cards with DS30X cables (up to 96 channels)

Figure 18: One MPB96 board and three MGate cards with CAT5 cables (up to 96 channels)



High capacity configuration

High capacity is available on the 1002rp, 1005r, and 1006r servers only. High capacity consists of three MPB96 boards, installed with six MGate cards, providing a capacity of up to 192 channels and 288 MPUs.

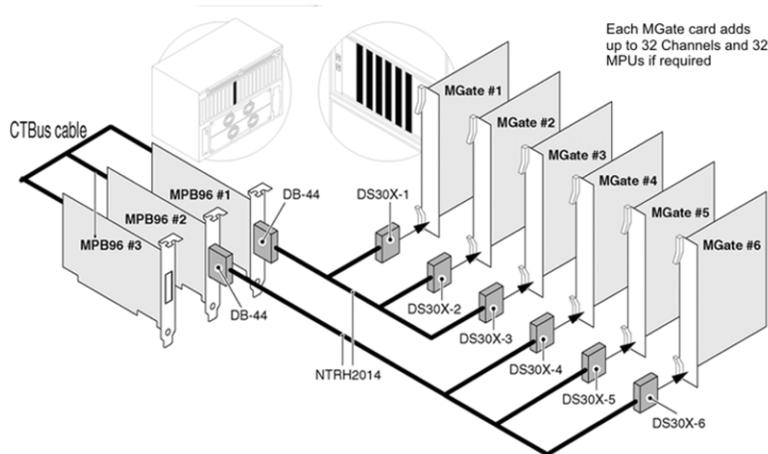


Figure 19: High capacity 3-MPB96 and 6-MGate

To install the DS30X cable for the MPB96 board

1. At the back of the Media Gateway or Media Gateway Expansion, locate the connector associated with the slot occupied by the MGate card. If you have an Option 11C cabinet, the connector is below the MGate card.
2. Attach the DS30X connector on the NTRH2014 cable to the slot connector as shown in the previous diagram.
 - a. Loosen the connector's Velcro fastening strap.
 - b. Connect the amphenol connector on the MGate cable to the connector on the back of the Media Gateway or Media Gateway Expansion.
 - c. Secure the connection by tightening the connector's retaining screw and Velcro fastening strap.

[Figure 20: DS30X cable connection to MPB96](#) on page 64 shows how to secure the MGate cable connection.

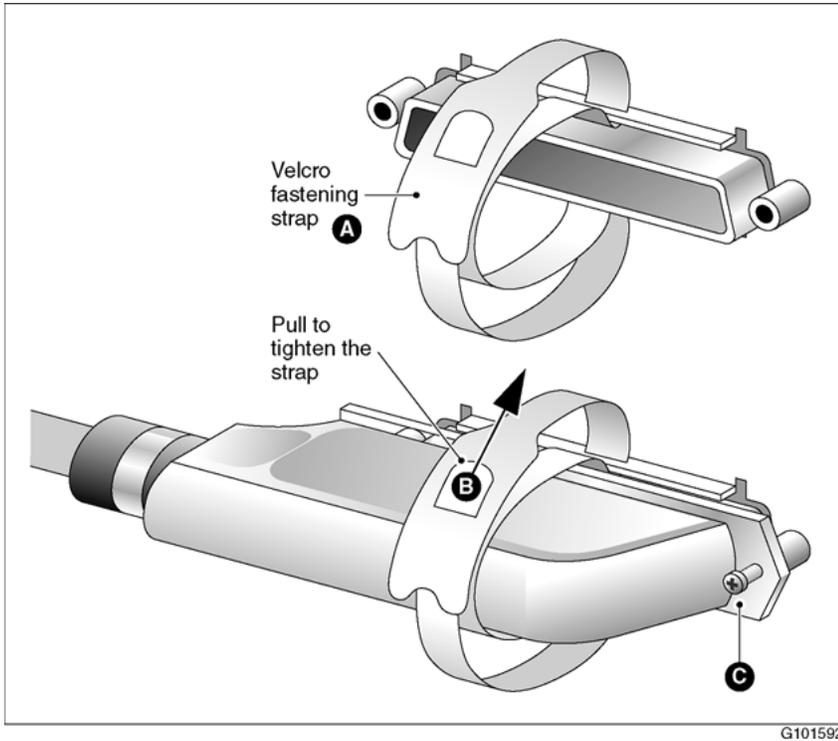
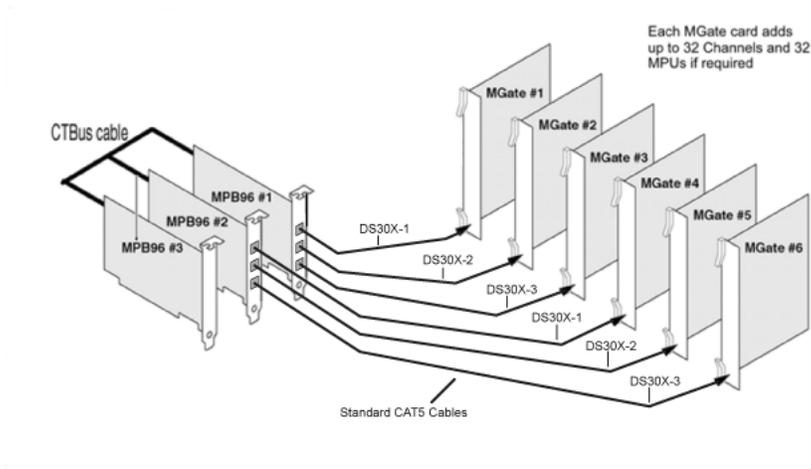


Figure 20: DS30X cable connection to MPB96

3. Connect the other end of the MGate cable to the MPB96 board's connector on the bottom of the CallPilot server.

Figure 21: High capacity 3-MPB96 and 6-MGate



To install the CAT5 cable for the MPB96 board

1. At the back of the Media Gateway or Media Gateway Expansion, locate the connector associated with the slot occupied by the MGate card. If you have an Option 11C cabinet, the connector is below the MGate card.
2. Connect the CAT5 cable connector to the front of the MGate card or to the Mertek adapter.
3. Connect the other end of the MGate cable to the MPB96 board's connector on the bottom of the CallPilot server.

MGate cabling to the NTRH40CAE5 MPB96 card (600r, 1005r, and 1006r)

Note that the RJ-45 connectors on the 600r MPB96 board are numbered from left to right.

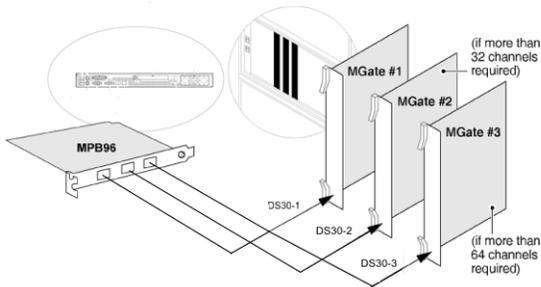


Figure 22: One MPB96 board and three MGate cards on the 600r (up to 96 channels)

Note that the RJ-45 connectors on the 1005r MPB96 board are numbered from right to left.

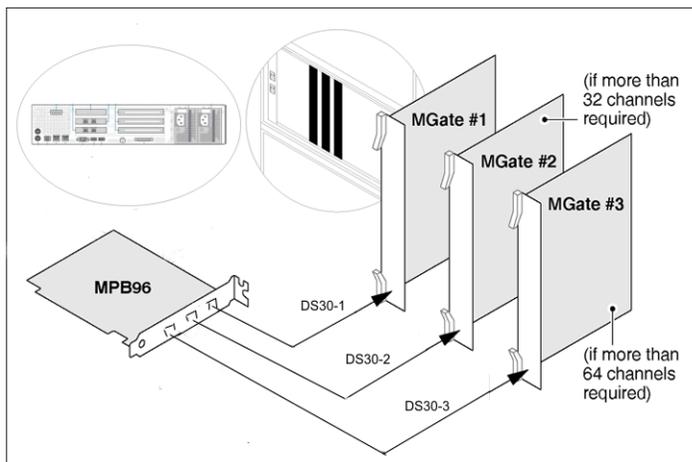


Figure 23: One MPB96 board and three MGate cards on the 1005r and 1006r (up to 96 channels)

High capacity configuration

High capacity using the NTRH40CAE5 MPB96 boards is available on the 1005r and 1006r servers only. High Capacity consists of three MPB96 boards, installed with six MGate cards, providing a capacity of up to 192 channels and 288 MPUs.

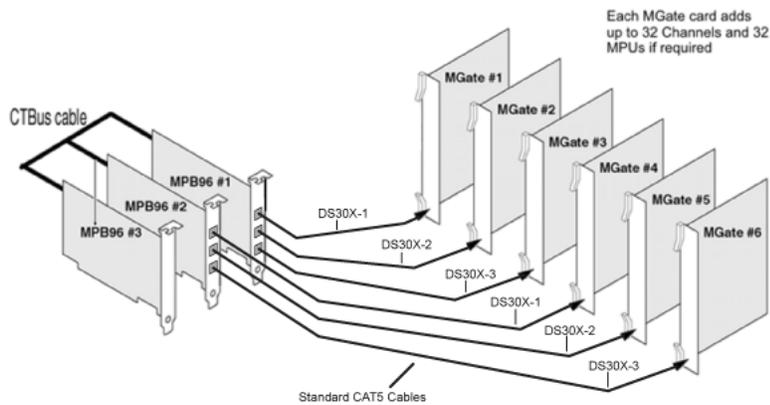


Figure 24: High capacity three MPB96 and six MGate

Connecting the DS30 cable to an MGate on the CS 1000S or CS 1000E

⚠ Caution:

Do not connect the CAT5 cable directly to RJ-45 connector on the MGate card, as this results in unacceptable levels of electromagnetic interference (EMI). Install the NTDU0609 cable to prevent excessive EMI as described in the following procedure.

1. Obtain an NTDU0609 cable. See the diagram below for an illustration of the cable.
2. Insert the RJ-45 connector at one end of the NTDU0609 cable into the RJ-45 connector on the MGate card.
3. Route the NTDU0609 cable through one of the cutouts on the side of the cabinet. Place one ferrite on each side of the cutout. See the diagram below.

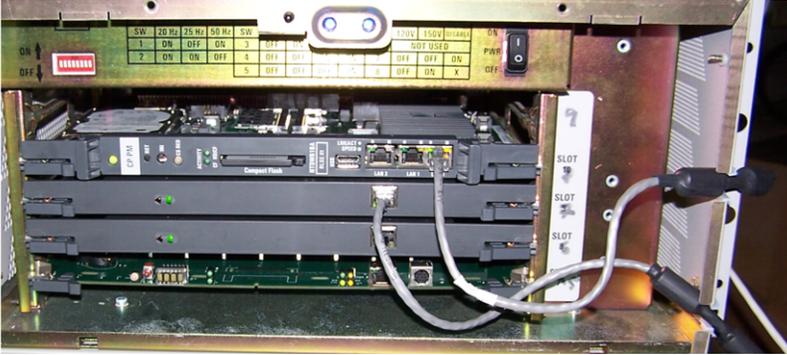


Figure 25: NTDU0609 cable routing

4. Connect the CAT5 cable to the NTDU0609 cable.
5. Route the CAT5 cable and connect it to the appropriate RJ-45 connector on the MPB96.

Connecting the CAT5 cable to an MGate card in the CS 1000M

⚠ Caution:

Do not connect the CAT5 cable directly to the RJ-45 connector on the MGate card, as this results in unacceptable electromagnetic interference (EMI).

1. Obtain a Merteck N0193176 50 pin Amphenol to RJ-45 adaptor.
2. At the rear of the Universal Equipment Module (UEM), locate the Amphenol connector associated with the MGate card.
3. Attach the Merteck N0193176 adaptor to the amphenol connector of the MGate card. (Either version of the adaptor can be used).
4. Connect one end of the CAT5 cable to the RJ-45 connector on the adaptor.
5. Route the CAT5 cable and connect it to the appropriate RJ-45 connector on the MPB96 board in the CallPilot server.

Connecting the CAT5 cable to an MGate card in the Option 11C Cabinet

⚠ Caution:

Do not connect the CAT5 cable directly to RJ-45 connector on the MGate card, as this results in unacceptable levels of electromagnetic interference (EMI). Install the NTDK8305 cable to prevent excessive levels of EMI as described in the following procedure.

1. Connect the NTDK8305 cable to the RJ-45 connector on the NTRB18DAE5 MGate card.
2. Run the NTDK8305 cable through the cable routing channel directly below the MGate card.
3. Fasten the NTDK8305 cable with a tie wrap to the cable routing channel lug.

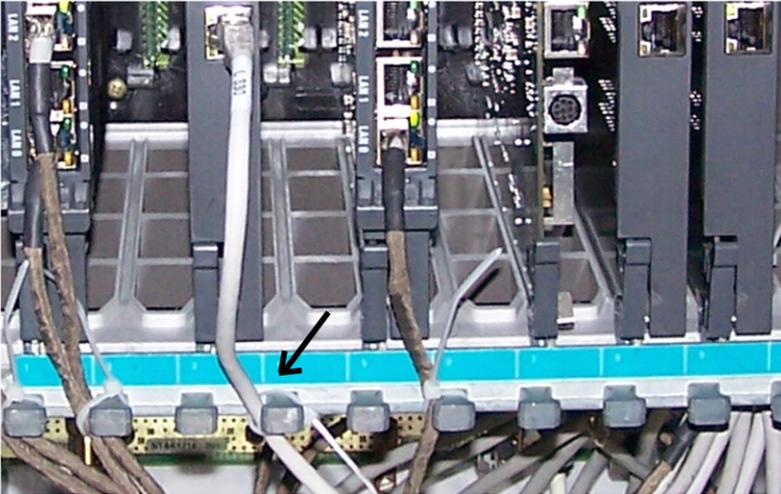


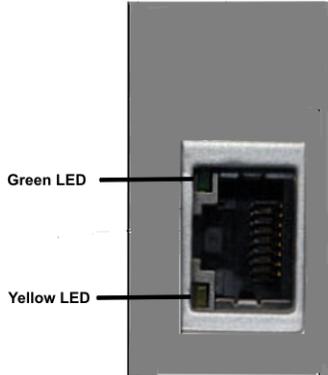
Figure 26: NTDK8305 cable routing

4. Find a suitable location as close as possible to the rear of the chassis on which to fasten the NTDK8305 cable with a tie wrap. This location must be a metallic part of the chassis.
5. Mark the NTDK8305 cable at the point where it is to be fastened to the chassis, and remove approximately two inches of sheathing from around the mark, exposing the braided shield.
6. Fasten the NTDK8305 cable to the chassis with a tie wrap. Ensure the exposed braided shield makes firm contact with the metal portion of the chassis.
7. Route the NTDK8305 cable through the rear of the chassis.
8. Connect the CAT5 cable to the female RJ-45 connector on the NTDK8305 cable.
9. Route the CAT5 cable and connect it to the appropriate RJ-45 connector on the MPB96.

When the NTRH2014 CAT5 cable is connected to the M1 switch (to the connector associated with the slot occupied by the CR MGate card), both LEDs (green & yellow) get turned OFF. This is old MGate emulation mode, both LED's on the CR-MGate RJ45 are turned OFF (no corresponding LED's on the old MGate). This is true whenever NTRH2014 cable attachment is detected regardless of whether the DS30 signal from original MPB96 is good or not, and also regardless of whether or not a CAT-5e cable is plugged into the faceplate.

NTRB18DAE5 MGate Link LED indications

When the DS30 cable is connected to the MGate card from the MPB96, the LEDs on the faceplate of the MGate card indicate the status of the DS30 link. The Link status LEDs are only operative when the MGate card is connected to the NTRH40CAE5 MPB96 board



Green LED	Link Status
On	Good DS30 signal from far end.
Off	No DS30 signal from far end

Yellow LED	Link Status
On (Blink)	Frame slip event.
On (steady)	No DS30 signal
Off	Normal

The logic flow and precedence order for the CR-MGate faceplate RJ-45 LED control is as follows:

1. Is an NTRH2014 cable attached to the backplane? If yes, go to step C, otherwise go to step 2.
2. Is an MerteK N0193176 adapter attached to the backplane? If yes, go to step 3. If no adapter (and no cable) is detected, go to step 4.
3. Is good Manchester encoded DS-30 signal input detected from the backplane? If yes go to step A. If no go to step B.
4. Is good Manchester encoded DS-30 signal input detected on faceplate RJ-45? If yes, go to step A. If no go to step B.

Step	Link status	CR-MGate RJ-45 green LED	RJ-45 yellow LED
A	Good DS-30 signal found	turn ON	turn OFF blink once for every frame slip
B	No DS-30 signal found	turn OFF	turn ON
C	Old MGate emulation mode	turn OFF	turn OFF



Important:

If an adapter (or NTRH2014 cable) is attached, the CR-MGate faceplate RJ-45 input is ignored.

What is next?

Continue with [Configuring the Avaya Communication Server 1000 system](#) on page 71.

Chapter 4: Configuring the Avaya Communication Server 1000 system

In this chapter

- [Avaya CS 1000 hardware and software requirements](#) on page 72
- [CS 1000 configuration checklist](#) on page 73
- [Provisioning the ELAN subnet](#) on page 76
- [Defining the Message Register for AML message tracing](#) on page 78
- [Configuring CS 1000 IP addresses and enabling the Ethernet interface](#) on page 79
- [Defining CallPilot in the customer data block](#) on page 82
- [Configuring the ACD agent queue](#) on page 86
- [Configuring ACD agents](#) on page 87
- [Enabling the card slots](#) on page 89
- [Defining the default ACD DN](#) on page 90
- [Configuring CDN queues for messaging services](#) on page 91
- [Configuring phantom DNs](#) on page 92
- [Configuring dummy ACD DNs](#) on page 96
- [Provisioning user phonesets](#) on page 97
- [Configuring the route data block for Network Message Service](#) on page 100
- [Saving CS 1000 changes](#) on page 101

Avaya CS 1000 hardware and software requirements

Required hardware

To support connectivity to tower and rackmount Avaya CallPilot® servers, you must install one or more MGate cards (NTRB18CA or NTRB18DAE5) in the Media Gateway or Media Gateway Expansion, as described in [Section A: Installing the MGate card](#) on page 39.



Important:

The 201i or 202i server does not use an MGate card (NTRB18CA or NTRB18DAE5).

Required CS 1000 system software

To support the Avaya CallPilot 201i or 202i server, the CS 1000 system requires software release X21 Release 3.0 or later.

To support the CallPilot 600r, 703t, 1002rp, 1005r, or 1006r servers, the CS 1000 system requires software release X21 Release 3.0 or later.

Required X21 PEPs

Check the CallPilot Distributor Technical Reference (DTR) at for required X21 PEPs.

You require a user name and password to access this site.

CS 1000 configuration checklist

Introduction

The following checklist provides a list of the tasks you must complete for correct CallPilot and CS 1000 system interoperation. Detailed instructions are provided for each task, as indicated, in the remainder of this chapter.

Table 13: Configuration checklist

Step	Overlay	See page	Check
1	Ensure that the ELAN subnet for the AML link and its associated VSID in the configuration record is defined. This provides the Ethernet connection over which AML messages are exchanged between the CS 1000 system and CallPilot.	17	Provisioning the ELAN subnet on page 76 <input type="checkbox"/>
2	Define the Message Register for AML message tracing.	17	Defining the Message Register for AML message tracing on page 78 <input type="checkbox"/>
3	If the CS 1000 system has not been defined with an IP address, configure it for the ELAN subnet interface.		Configuring CS 1000 IP addresses and enabling the Ethernet interface on page 79 <input type="checkbox"/>
4	Enable the ELAN subnet link.	137	Configuring CS 1000 IP addresses and enabling the Ethernet interface on page 79 <input type="checkbox"/>
5	Enable the ELAN subnet connection.	48	Configuring CS 1000 IP addresses and enabling the Ethernet interface on page 79 <input type="checkbox"/>
6	Define CallPilot in the customer data block with the Call Park Allowed (CPA) and	15	Defining CallPilot in the customer data block on page 82 <input type="checkbox"/>

Step	Overlay	See page	Check
			Message Center Included (MCI) options enabled. Also define in the customer data block how unanswered and busy calls are routed.
7	16	1 on page 85	<input type="checkbox"/>
8	23	Configuring the ACD agent queue on page 86	<input type="checkbox"/>
9	11	Configuring ACD agents on page 87	<input type="checkbox"/>
10	32	Enabling the card slots on page 89	<input type="checkbox"/>
11	23	Defining the default ACD DN on page 90	<input type="checkbox"/>
12	23	Configuring CDN queues for messaging services on page 91	<input type="checkbox"/>
13	97	Configuring phantom DNs on page 92	<input type="checkbox"/>
14	10 or 23	Configuring phantom DNs on page 92 or Configuring dummy ACD DNs on page 96	<input type="checkbox"/>

Step	Overlay	See page	Check
15	Provision user phonesets to support CallPilot. Notes: <ul style="list-style-type: none"> • To determine which phonesets are supported by the CS 1000 system, see the Communication Server 1000S: Installation and Configuration. • For instructions on provisioning i2004 phonesets, see Software Input/Output: Administration. 	10 or 11 Provisioning user phonesets on page 97	<input type="checkbox"/>
16	If you purchased Network Message Service, configure the route data block.	Configuring the route data block for Network Message Service on page 100	<input type="checkbox"/>
17	Save the configuration changes.	Saving CS 1000 changes on page 101	<input type="checkbox"/>
18	If you made changes to the ELAN subnet interface configuration in step 3 of this checklist, perform a CS 1000 INI after you have saved the configuration changes (as instructed in step 17 of this checklist).	n/a	<input type="checkbox"/>
19	To avoid voice channel blocking, see the Communication Server 1000 Engineering Guide to determine placement of MGate cards.	n/a	

**Note:**

You can also print configuration information from overlay 20 at any time.

How the overlays are presented in this chapter

Overlays are programmed by responding to a series of prompts. The procedures in this section mention only those prompts that require a specific entry for CallPilot.

You can program other prompts if necessary for your site. To accept the default value for other prompts, press Enter.

 **Important:**

Ensure that you update the CS 1000 database when you finish making changes, as described in [Saving CS 1000 changes](#) on page 101.

Working with overlays

When you work with overlays, follow these general steps:

1. Load the appropriate overlay.
2. Respond to the prompts as shown in the tables in this section. Press Enter after each prompt until you reach the next one that you must define for CallPilot.
3. When you complete the configuration, type **** in response to the REQ prompt.

The customer number

CallPilot can only be provided on a per customer basis on the CS 1000 system. AML messages used for communications between the CS 1000 system and CallPilot contain a customer number to which CallPilot belongs.

 **Important:**

When you type the customer number in the overlays, ensure that it is the correct customer number.

Provisioning the ELAN subnet

Introduction

Define and configure the ELAN subnet for the AML link and its associated VSID in the configuration record. This provides the Ethernet connection over which AML messages are exchanged between the CS 1000 system and CallPilot.

To provision the ELAN subnet

1. Load overlay 17.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Action device and number
ADAN	NEW ELAN xx	Configure a new link and assign it a number, where xx is within the ELAN subnet range (16-31). You can use any number in this range as long as it is not already used.
CTYP	ELAN	Card type
DES	x...x	type a designator to identify this ELAN subnet.
REQ	CHG	Change
TYPE	VAS	Value added server configuration
VAS	new	Configure a new AML link or change the existing link configuration.
VSID	yy	The VAS identifier can be in the range of 16-31. For convenience, this can be the same number you assigned to the new ELAN subnet link (in response to the ADAN prompt).
ELAN	xx	This should be the same number defined in ADAN.
SECU	x...x	If you have Contact Center connected to your switch, choose YES (even if you are not using Contact Center Voice Services Support).
REQ	CHG	Change
TYPE	PARM	System parameters
NCR	x...x	Number of call registers (range depends on system type). Increment the current value by 2 x the number of CallPilot DS0 channels. For example, if the current NCR value is 500 and there are 24 DS0 channels, change the NCR value to 548.

Prompt	Response	Description
CSQI	(20) to 255	Maximum number of call registers for CSL input queues. Set this parameter to 2 x the number of CallPilot DS0 channels. For example, if there are 24 DS0 channels, type 48.
CSQO	(20) to 255	Maximum number of call registers for CSL/AML output queues. Set this parameter to 2 x the number of CallPilot DS0 channels. For example, if there are 24 DS0 channels, type 48.
	<Enter>	Press Enter until you reach the end of the overlay (REQ prompt).
REQ	****	Exits the overlay.

Defining the Message Register for AML message tracing

Introduction

This section provides instructions for updating the Message Register (MGCR) parameter. The MGCR parameter affects the AML output when message tracing is turned on for the ELAN subnet.

 **Important:**

The MGCR parameter is used by your Avaya customer support representative to troubleshoot your CallPilot and CS 1000. This parameter is not required for normal day-to-day CallPilot operation.

To define the MGCR parameter

1. Load overlay 17.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	CHG	Change
TYPE	PARM	System parameters

Prompt	Response	Description
MGCR	0 to NCR	Maximum number of call registers used by AUX messaging. The recommended value for CallPilot is 25.
REQ	****	Exits the overlay.

Configuring CS 1000 IP addresses and enabling the Ethernet interface

Introduction

If the CS 1000 system has not been defined with the necessary IP address information (see below), configure the IP addresses for the Ethernet interface. You must also enable the Ethernet interface, as described in this section.

Notes:

- The CS 1000 system has dual CPUs.
- If the CS 1000 system is also connected to a Avaya Server Subnet (NS Subnet), you must define a gateway IP address.



Important:

To change an IP address after CallPilot is installed and running, you must do the following:

- 1 Courtesy stop and shut down CallPilot.
- 2 Change the IP addresses on the switch, as described in this section.
- 3 Restart CallPilot.
- 4 Rerun the CallPilot Configuration Wizard to update the switch IP address information.

To configure the IP addresses and enable the Ethernet interface

The following data is used in examples in this procedure:

Data	Value (examples only)
Primary IP address	47.1.1.10
Primary Host Name	PRIMARY_HOST
Subnet mask	255.255.255.0
Default gateway IP address	47.1.1.1
Network IP address	0.0.0.0

1. Load overlay 117.
2. Perform the following substeps to check the current IP addresses to see if they already match what you plan to configure for CallPilot.

If the current values displayed by the following commands must be updated, then continue with the remaining steps in this procedure. Otherwise, go to step 15.

- a. Type PRT HOST and press Enter.
- b. Type STAT HOST and press Enter.
- c. Type PRT MASK and press Enter.
- d. Type PRT ELNK and press Enter.

3. Load overlay 137.
4. Type DIS ELNK and press Enter.
5. Type STAT ELNK and press Enter.
6. Confirm that the system displays ELNK DISABLED.
7. Load overlay 117.
8. Create a host entry for the primary IP address by typing the following command:
 NEW HOST NAME xxx.xxx.xxx.xxx (where NAME is the host name for the primary IP address, and xxx.xxx.xxx.xxx is the primary IP address)
 Example: NEW HOST PRIMARY_HOST 47.1.1.10
9. If the CS 1000 system is connected to an Avaya Server Subnet (NS Subnet), create a host entry for the gateway IP address by typing the following command:
 NEW HOST NAME xxx.xxx.xxx.xxx (where NAME is the host name for the gateway IP address, and xxx.xxx.xxx.xxx is the gateway IP address)
 Example: NEW HOST GATEWAY 47.1.1.1
10. Assign a host to the primary IP address by typing the following command:
 CHG ELNK ACTIVE NAME (where NAME is the host name for the primary IP address)
 Example: CHG ELNK ACTIVE PRIMARY_HOST (entry for primary host)

11. Set up the Ethernet subnet mask by typing the following command:
CHG MASK xxx.xxx.xxx.xxx (where xxx.xxx.xxx.xxx is the subnet mask)
Example: CHG MASK 255.255.255.0
12. If using a gateway, ensure that the routing entry is set up and enabled. If the route has been set up previously, go to step 13. Otherwise, set up and enable the routing entry as follows:

Set up the routing entry by typing the following command:
NEW ROUTE xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy (where xxx.xxx.xxx.xxx is the network IP address and yyy.yyy.yyy.yyy is the gateway IP address; put one space between the network IP address and the gateway IP address)
Example: NEW ROUTE 0.0.0.0 47.1.1.1

Enable the route by typing the following command:
ENL ROUTE x (where x is the number assigned to the ROUTE entry)
13. Update the INET database by typing the following command:UPDATE DBS
14. Type **** and press Enter to exit the overlay.
15. Load overlay 137.
16. Type STAT ELNK and press Enter.
17. If the system displays ELNK ENABLED, then go to step 18. If the system displays ELNK DISABLED, then do the following substeps:
 - a. Type ENL ELNK and press Enter.
 - b. Type STAT ELNK and press Enter.
 - c. Confirm that the system displays ELNK ENABLED. Then go to step 18.
18. Load overlay 48.
19. Type STAT ELAN and press Enter.
20. If the system displays ELAN ENABLED, then go to step 21. If the system displays ELAN DISABLED, then do the following substeps:
 - a. Type ENL ELAN and press Enter.
 - b. Type STAT ELAN and press Enter.
 - c. Confirm that the system displays ELAN ENABLED. Then go to step 21.
21. Load overlay 117.
22. Verify the changes as follows:
 - a. Type PRT HOST and press Enter.
 - b. Type STAT HOST and press Enter.

- c. Type PRT MASK and press Enter.

Defining CallPilot in the customer data block

Introduction

You must define the CallPilot service in the customer data block, with the Call Park Allowed (CPA) and Message Center Included (MCI) options enabled.

During this configuration, you also define how unanswered and busy calls are routed:

- Flexible Call Forward (FNAD/FNAN/FNAL) is set on a per customer basis. Define the call forward DN in the user's phoneset data.
- Call Forward No Answer/Busy (MDID/NDID/MWFB) is set on a per customer basis. All no answer and busy calls are routed to the flexible call forward DN, provided that the called phoneset has the Message Waiting Allowed (MWA) class of service enabled.

Normally, non-Direct Inward Dialing (DID) calls are routed to CallPilot when a no answer or busy condition is encountered. As an option, you can route DID calls to the attendant's or user's Hunt DN.

To modify the customer data block

1. Load overlay 15.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	CHG	Change
TYPE	FTR	Customer features and options
CUST	xx	Customer number (0-99)
OPT	CPA MCI	Call Park Allowed and Message Center Included are enabled for the customer.
IDEF	YES or NO	Internal/External Definition Set to YES if the Call Forward by Call Type feature (CFCT) is enabled on the CS 1000 system.

3. Load overlay 15 again, and then for each prompt listed below, type the response indicated:

Prompt	Response	Description
REQ	CHG	Change
TYPE	ATT	TYPE Attendant consoles
CUST	xx	Customer number (0-99) AQTT 1-255 (30) Attendant Queue Timing Threshold in seconds
ATDN	(0) yyyy	Attendant DN
MATT	NO (YES)	Set to YES if Network Message Service (NMS) has not been purchased. If NMS has been purchased, set the primary CS 1000 system to YES and all secondary systems to NO.
AQTT	1-255 (30)	Attendant Queue Timing Threshold in seconds
AODN	CallPilot CDN	Attendant Overflow DN. Set this prompt to a CallPilot CDN to launch a CallPilot service when the attendant overflows. The SDN Table in CallPilot must have the desired AODN service defined for DN 0. The CS 1000 system issues an SCH1872 error, but accepts the DN. This error is a warning that the DN must be a CallPilot CDN.

4. Load overlay 15 again, and then for each prompt listed below, type the response indicated:

Prompt	Response	Description
REQ	CHG	Change
TYPE	RDR	Call Redirection
CUST	xx	Customer number (0-99)
FNAD	FDN	Call forward no answer DID calls are routed to flexible CFNA DN.
FNAN	FDN	Call forward no answer non-DID calls are routed to flexible CFNA DN.
AODN	CallPilot CDN	Attendant Overflow DN. Set this prompt to a CallPilot CDN to launch a CallPilot service when the attendant overflows. The SDN Table in CallPilot must have the desired AODN service defined for DN 0. The CS 1000 system issues an SCH1872 error, but accepts the DN. This error is a warning that the DN must be a CallPilot CDN.

Prompt	Response	Description
FNAL	FDN	Call forward no answer local calls (with CFCT enabled) are routed to flexible CFNA DN.
CFNA, CFN0, CFN1, CFN2	4	The number of ring cycles before the call is forwarded. The prompts CFN0, CFN1, and CFN2 may appear instead of CFNA, depending on the release installed on the CS 1000 system. see your CS 1000 system X21 documentation for details.

5. Load overlay 15 again, and then for each prompt listed below, type the response indicated:

Prompt	Response	Description
REQ	CHG	Change
TYPE	FTR	
CUST	xx	Customer number (0-99)
EEST	(NO) YES	Customer features and options The originating party does not receive DTMF feedback. Set remote CS 1000 sites to NO.

6. Load overlay 15 again, and then for each prompt listed below, type the response indicated:

Prompt	Response	Description
REQ	CHG	Change
TYPE	NET	Networking
CUST	xx	Customer number (0-99)
ISDN	(NO) YES	Set to YES only if NMS has been purchased. Otherwise, set to NO.
PNI		NMS only. The Private Network Identifier. Within one network, use the same PNI value in overlays 15 and 16. When you interwork with different networks, type the PNI of this CS 1000 system in overlay 15, and the PNI of the remote CS 1000 system in overlay 16.
HLOC		NMS only. Home Location Code (ESN) of the CS 1000 system. This can be in the range 100-999.
LSC		NMS only. Local Steering Code (established in the Coordinated Dialing Plan, or CDP) of the CS

Prompt	Response	Description
		1000 system. This prompt only appears for 5- or 6-digit dialing plans.
	<Enter>	Press Enter until you reach the end of the overlay (REQ prompt).
REQ	****	Exits the overlay.

Additional steps to support the Call Forward by Call Type feature

The Call Forward by Call Type (CFCT) feature is installed as part of the base X21 software.

1. Load overlay 16.
2. For each prompt listed below, type the response indicated.
3. For those prompts that are not listed, you can accept the default by pressing Enter.
4. IDEF must be set to YES in overlay 15 to support CFCT and for the IDEF prompt to appear in overlay 16 (see [To modify the customer data block](#) on page 82).:

Prompt	Response	Description
REQ	NEW or CHG	
TYPE	RDB	Route data block
CUST	xx	Customer number (0-99)
ROUTE		Route number
RCLS	EXT	Route class is marked as external.
IDEF	LOC	Use local data to define a call as internal or external.
	<Enter>	Press Enter until you reach the end of the overlay (REQ prompt).
REQ	****	Exits the overlay.

Configuring the ACD agent queue

Introduction

You must set up only one ACD agent queue to service CallPilot, unless you are enabling the Contact Center Voice Services Support feature (see "Contact Center Voice Services Support additional requirements" below). This queue holds all the agents that correspond to DS0 channels on the CallPilot server.

Contact Center Voice Services Support additional requirements

If you are enabling the Contact Center Voice Services Support feature, you must set up two additional ACD agent queues: one for ACCESS ports, and one for IVR ports. A segment of the CallPilot ports must be dedicated to the Contact Center Voice Services Support feature.

To configure an ACD agent queue

1. Load overlay 23.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	ACD	Indicates this is an ACD queue.
CUST	xx	Customer number (0-99)
ACDN	yyyy	This is the ACD DN for CallPilot.
MWC	NO	Message Waiting Center
MAXP	zzzz	Maximum number of agents. MAXP must be equal to or greater than the total number of multimedia channels installed on your system.
IVR	YES	Interactive Voice Response queue
CALP	POS or TER	Called Party DN POS - Sends the POSID +DNIS in the called Party DN field in the PCI

Prompt	Response	Description
		message TER - Sends the terminating DN in the called Party DN field in the PCI message
ALOG	YES	Provide automatic logon for ACD agents.
	<Enter>	Press Enter until you reach the REQ prompt.
REQ	****	Exits the overlay.

Configuring ACD agents

Introduction

For CallPilot, you must define channels as ACD agents on M2008 digital sets. All agents are added to the ACD queues that you have configured.

Each agent must have the VCE and MMA class of service. To get the VCE class of service on the upper 16 units (15 to 31), you must first specify the FLXA class of service. Each agent must be provisioned with the following feature keys: ACD, SCN, NRD, MSB, TRN, and AO3.

 **Note:**

You can define a more restrictive class of service for the agents (for example, Conditionally Toll Denied [CTD]). Call restrictions in effect for the class of service take precedence over the dialing restrictions and permissions provided by CallPilot.

Terminal numbers

A Terminal number (TN) is required for each agent.

Integrated server (201i or 202i server)

For the 201i or 202i server, ACD agents use TNs associated with the slot location of the 201i or 202i server.

*** Note:**

The left card slot used by the TNs must be used first.

*** Note:**

The 202i occupies two slots, but uses only the left slot is used by the TNs.

Tower or rackmount servers

For the tower and rack versions of the CallPilot server, ACD agents use TNs associated with the slot location of the MGate card (NTRB18CA or NTRB18DAE5).

Position IDs

You also need a Position ID for each agent. The server uses the position ID to inform the CS 1000 system to which agent an incoming call should be routed.

For ease of maintenance, assign sequential numbers to the IDs that are not already in use.

To configure agents

1. Load overlay 11.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW	
TYPE	2008	ARIES digital set with 8 programmable keys.
TN	c u	Terminal number of the MGate card (tower and rack server), or the 201i or 202i server, where c is the card, and u is the unit.
CUST	xx	Customer number (0-99)
CLS	WTA UNR VCE MMA (units 0-15) FLXA VCE MMA (units 16-31)	Voice terminal, Multimedia Agent, Flexible voice/data allowed.

Prompt	Response	Description
key	0 acd xxxx 0 yyyy	where xxxx is the ACD DN of the CallPilot agent queue, and yyyy is the Position ID of the agent.
key	1 scn zzzz	where zzzz is the single-call nonringing DN used to make outbound calls.
key	2 msb	Make Set Busy
key	3 nrd	Not Ready
key	4 trn	Transfer
key	5 ao3	Three-Party Conference
AST (For IVR & Access Agents only)	0 1	If you are enabling the Contact Center Voice Services Support feature, you must define 0 and 1 as the AST key 0 and key 1 values. If you are not enabling the Contact Center Voice Services Support feature, then press Enter to skip this prompt.
	<Enter>	Press Enter until you reach the end of the overlay (the REQ prompt).
REQ		If you are finished adding agents, type **** to exit the overlay. To add another agent, return to the top of the table.

Enabling the card slots

Introduction

After you have configured the ACD agents, use overlay 32 to ensure that the card slots used by an MGate card (NTRB18CA or NTRB18DAE5) or 201i or 202i server are enabled.

 **Note:**

The left card slot used by the TNs must be used first.

 **Note:**

The 202i occupies two slots, but uses only the left slot is used by the TNs.

To enable the card slots

 **Note:**

This procedure uses the syntax STAT n and ENLC n.

1. Load overlay 32.
2. Type STAT n and press Enter, where n is the card slot used by an MGate card or the 201i or 202i server.

Result: The status of the ACD agents defined for this slot appears. If the ACD agents are disabled, then enable the card slot.

3. Type ENLC n and press Enter, where n is the card slot used by an MGate card or the 201i or 202i server.
4. To verify that the card slot and the ACD agents are enabled, type STAT n and press Enter, where n is the card slot used by an MGate card or 201i or 202i server.

Result: The status of the ACD agents defined for this slot appears.

5. Repeat this procedure for all other card slots used by an MGate card or the 201i or 202i server.

Defining the default ACD DN

Introduction

Before you configure the CDN queue, define the default ACD DN that needs to be referenced in the CDN. During normal operation, the CDN is in control mode, and callers are queued to be routed and then answered by CallPilot services. Under error conditions (for example, if the AML link is down), the CDN operates in default mode and calls are routed to the default ACD DN defined for the CDN. This section describes how to set up the default ACD DN so that these calls are handled by the attendant.

For the attendant to process incoming calls to CallPilot when the CDN is in default mode, define a dummy ACD DN and set it to night call forward to the attendant.

To create a default ACD DN

1. Load overlay 23.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW	
TYPE	ACD	
CUST	0	Customer number (0-99)
ACDN	xxxx	The ACD DN. Enter this DN as the DFDN in the CDN configuration.
MWC	NO	Message Waiting Center. Set to NO.
MAXP	1	This indicates that there are no agents in this queue and it is, therefore, a dummy queue.
NCFW	0	Night call forward to the attendant.
	<Enter>	Press Enter until you reach the end of the overlay (the REQ prompt).
REQ	****	Exits the overlay.

Configuring CDN queues for messaging services

Introduction

Configure the following CDN queues:

- Configure a primary CDN for Voice Messaging. This becomes the main CDN queue.
- Configure a secondary CDN for Multimedia Messaging, if you want to provide users with fax capability.

 **Note:**

Avaya strongly recommends that you use either a phantom DN or a dummy ACD DN for all other messaging services.

To configure a CDN queue

1. Load overlay 23.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW	
TYPE	CDN	Control DN queue
CUST	xx	Customer number (0-99)
CDN	yyyy	The Control DN of the queue. This number must be entered as the SDN for the messaging service in the SDN Table.
DFDN	zzzz	The default ACD DN (see page 115). Calls to the CDN are directed to this ACD DN if the link or CallPilot goes down. Avaya recommends that this is not defined as the ACD DN of the CallPilot ACD queue.
VSID	<Enter>	Press Enter so that the ID is dynamically assigned to the CDN when the ELAN subnet link is established.
	<Enter>	Press Enter until you reach the end of the overlay (the REQ prompt).
REQ		To configure another CDN, return to the top of the table. To exit, type ****.

Configuring phantom DNs

Introduction

There are two reasons for configuring phantom DNs on the switch:

- to create dialable numbers for CallPilot services
- to create virtual fax DNs for users who want a separate fax number

 **Important:**

Another option is to configure dummy ACD DNs instead of phantom DNs. See [Configuring dummy ACD DNs](#) on page 96.

Supporting multiple languages

For Fax Item Maintenance, Voice Item Maintenance, Speech Activated Messaging, and Paced Speech Messaging, you might have purchased multiple language support.

This means that, for example, you can create an English and a Spanish version of Voice Item Maintenance if you have these languages installed. To support this, you must create a phantom DN for each supported language.

Therefore, in this case, you need two phantom DNs (one for English Voice Item Maintenance and one for Spanish Voice Item Maintenance). This also means that callers must dial a different number to access the service, based on the language they prefer.

Virtual fax DNs for users with fax capabilities

Users who have fax capabilities can have one DN that serves as both their regular extension number and their fax number. In this case, you set up a phone for the user as described in [Provisioning user phonesets](#) on page 97. The user's phone must be forwarded to the Multimedia Messaging CDN.

However, some users may require two separate DNs—one DN that serves as their regular telephone number, and a second DN that serves as their fax number. For these users, you cannot simply define the virtual fax DN as another DN on the user's phoneset. Instead, you must set up a TN as the virtual fax DN. Because physical TNs are more costly, Avaya recommends that you configure phantom DNs instead.

A separate TN is necessary because a single TN (the telephone) can be call forwarded to only one DN (regardless of how many DNs appear on that phone). For these users, you must ensure that their telephone number (the mailbox DN) forwards to the Voice Messaging CDN, whereas their fax number (the virtual fax DN) forwards to the Multimedia Messaging CDN.

 **Note:**

When you add the user to CallPilot (as a mailbox owner), you must define this virtual fax DN as one of the user's extension DNs.

To check for existing phantom loops

A phantom loop must exist before you begin to configure phantom DN's. Use overlay 22 to print the configuration record to see if any phantom loops are already configured. A phantom loop is shown with the prefix "P", illustrated in this example:

 **Note:**

You can use superloops as phantom loops.

```
.
CEQU
MPED 8D
SUPL 000 004 008 012
016 032 036 040
048 P064 P068 (phantom loops 64 and 68)
DDCS
.
.
```

If no phantom loops are configured, then continue with [To configure a phantom superloop](#) on page 94. If a phantom loop is configured, then go to [To configure a phantom DN](#) on page 95.

To configure a phantom superloop

1. If no phantom loops are configured, load overlay 97.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	CHG	
TYPE	SUPL	Superloop
SUPL	Nxxx	Prefix the loop number with N to create a phantom loop. The loop number range is 96-112 in multiples of 4 (corresponds to slots 61- 80).
	<Enter>	Press Enter until you reach the end of the overlay (the REQ prompt).
REQ	****	Exits the overlay.

To configure a phantom DN

1. Load overlay 10.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW	
TYPE	500	PBX set type
TN	c u	Terminal number, where c is the card, and u is the unit. PHANTOM is echoed by the switch when the specified loop is phantom.
CDEN	xx	The card density supported by the loop, where xx can be DD - double density 4D - quadruple density
DN	yyyy	The DN must be single appearance.
CLS	WTA UNR	Unrestricted. Phantom DNs cannot originate calls, so this option is secure.
FTR	DCFw nn xxxx	DCFw = Default Call Forward nn = maximum number of digits in the DCFw DN xxxx = the CDN to which this DN forwards If this phantom DN is for a voice service, type the Voice Messaging CDN. If this phantom DN is for a fax service, type the Multimedia Messaging CDN. If this phantom DN is a virtual fax DN for a user, type the Multimedia Messaging CDN.
	<Enter>	Press Enter until you reach the end of the overlay (REQ prompt).
REQ		If you are finished adding phantom DNs, type **** to exit. To add another DN, return to the top of the table.

Configuring dummy ACD DN

Introduction

As an alternative to creating phantom DNs for directly dialable services, you can create a dummy ACD DN that is set up to call forward to the appropriate CDN depending on the multimedia channel type required.

Example

- For a service that requires only voice capability, forward the dummy ACD DN to the Voice Messaging CDN.
- For a service that requires fax capability, forward the dummy ACD DN to the Multimedia Messaging CDN.

To configure dummy ACD DNs

1. Load overlay 23.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW	
TYPE	ACD	
CUST	xx	Customer number (0-99)
ACDN	xxxx	Enter the DN for the service.
MWC	YES or NO	Message Waiting Center. If the CallPilot server is a Network Message Service (NMS) satellite site, set to YES. Otherwise, set to NO.
MAXP	1	This indicates that there are no agents in this queue and it is, therefore, a dummy queue.
NCFW	yyyy	Specify the appropriate CDN depending on multimedia channel type required (Voice

Prompt	Response	Description
		Messaging CDN or Multimedia Messaging CDN).
	<Enter>	Press Enter until you reach the end of the overlay (the REQ prompt).
REQ	****	Exits the overlay.

Provisioning user phonesets

Introduction

You must set up users' phonesets in a certain way to support CallPilot. The procedure depends on whether you are provisioning a digital phoneset or a 500 phoneset.

Required features

You must set up phonesets to support the following features:

- Call forward no answer to the appropriate CDN (voice or multimedia)

 **Note:**

You cannot forward users' phonesets to the Speech Activated Messaging CDN because this service does not provide call answering functionality.

- Call forward busy to the appropriate CDN
- Call forward all calls to the appropriate CDN
- Message Waiting key with the appropriate CDN as the Message Center DN

 **Note:**

If you do not plan to give fax capability to the user's mailbox, use the Voice Messaging CDN. If you plan to give fax capability to the user's mailbox, then use the Multimedia Messaging CDN.

To provision digital phonesets

1. Load overlay 11.
2. For each prompt listed below, type the response indicated in overlay 11. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW or CHG	
TYPE	2317, 2008, and so on	Type of set.
TN	c u	Terminal number of the phone, where c is the card, and u is the unit.
CUST	xx	Customer number (0-99)
FDN	yyyy	Flexible call forward no answer DN. Set this to the CDN of the Voice Messaging or Multimedia Messaging CDN queue.
HUNT	zzzz	Hunt (internal). Set this to the CDN of the Voice Messaging or Multimedia Messaging CDN queue.
CLS	WTA, UNR, FNA, FBA, HTA, MWA	Call forward no answer allowed. Call forward busy allowed. Hunt allowed. Message waiting allowed.
KEY	0 SCR xxxx	Single call ringing DN, where xxxx is the user's DN.
CPND	New	Calling Party Name Display (if adding a new set).
NAME	First,Last	The name of the phoneset user.
KEY	3 MSB	Make set busy
KEY	4 TRN	Transfer
KEY	5 AO3	Three-party conference. Required by the Call Sender feature.
KEY	6 CFW nn xxxx	Call forward all calls, where nn is the maximum number of digits in the Call Forward DN, and xxxx is the Voice Messaging or Multimedia Messaging CDN.
KEY	8 MWK yyyy	Add a message waiting key/lamp, where yyyy is the Voice Messaging or Multimedia Messaging CDN.
	<Enter>	Press Enter until you reach the end of the overlay (the REQ prompt).

Prompt	Response	Description
REQ		If you are finished adding phonesets, type **** to exit. To add another phoneset, return to the top of the table.

To provision 500/2500 phonesets

1. Load overlay 10.
2. For each prompt listed below, type the response indicated in overlay 10. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW	
TYPE	500	500 phoneset
TN	c u	Terminal number of the phone, where c is the card, and u is the unit.
CUST	xx	Customer number (0-99)
DN	yyyy	Directory number
HUNT	zzzz	Hunt (internal). Set this to the CDN of the Voice Messaging or Multimedia Messaging CDN queue.
CLS	WTA, UNR, HTA, MWA, FNA, FBA, XFA, LPA, DTN	Hunt allowed. Message waiting allowed. Call forward no answer allowed. Call forward busy allowed. MWI lamp is equipped (if not equipped, users are notified of new messages by interrupted dial tone).
FTR	FDN xxxx	Flexible call forward no answer. Set this to the Voice Messaging or Multimedia Messaging CDN.
FTR	CFW yy	Call forward all calls, where yy is the maximum DN length that users can specify as the call forward DN.
	<Enter>	Press Enter until you reach the end of the overlay (the REQ prompt).
REQ		If you are finished adding phonesets, enter **** to exit. To add another phoneset, return to the top of the table.

Configuring the route data block for Network Message Service

Introduction

If you have purchased Network Message Service (NMS) to allow a number of switches to share CallPilot (installed on only one switch), then configure the route data block. This section provides instructions for this step.

For details on additional switch configuration for NMS, see the "Configuring the switches" chapter in the *CallPilot Network Planning Guide* (NN44200-201).



Note:

Ensure that Digit Manipulation (DMI in overlay 86) is not used to insert ESN access codes at the sending switch. ESN access code insertion must be done at the receiving switch (INAC in overlay 16).

To modify the route data block

1. Load overlay 16.
2. For each prompt listed below, type the response indicated. For those prompts that are not listed, you can accept the default by pressing Enter.

Prompt	Response	Description
REQ	NEW or CHG	
TYPE	RDB	Route data block
CUST	xx	Customer number (0-99)
ROUTE		Route number
PNI		Customer Private Network ID of the non-local target CS 1000 system
NCRD	Yes	Network call redirection provides the CLID display information.
TRO	Yes	Optimize trunk usage on this route.
INAC	Yes	Insert an ESN access code to incoming private network calls.

Prompt	Response	Description
	<Enter>	Press Enter until you reach the end of the overlay (REQ prompt).
REQ	****	Exits the overlay.

Saving CS 1000 changes

Introduction

Once you modify the switch configuration to support CallPilot, save all changes to disk.

To save the configuration

1. Load overlay 43.
2. At the next "." prompt, type BKO to dump the data to disk.

Result: The system displays the data being saved. The following message appears:

RECORD COUNT=xxxx

DATADUMP COMPLETE

3. Return to step 2, and repeat this step two more times.

Use a new disk each time.

Important:

Do not remove the disk while the LED is lit. As long as the LED is on, the disk is still being written to.

What is next?

Continue with [Configuring the Avaya CallPilot® server software](#) on page 103.

Chapter 5: Configuring the Avaya CallPilot® server software

In this chapter

[Overview](#) on page 103

[Logging on to Windows 2003 on the CallPilot server](#) on page 105

[Running the Setup Wizard](#) on page 106

[Logging on to the CallPilot server with CallPilot Manager](#) on page 107

[Running the Configuration Wizard](#) on page 111

[Changing pcAnywhere caller passwords](#) on page 114

[Setting Remote Desktop Policy on a Server](#) on page 115

[Configuring CallPilot to operate in a Windows 2000 or 2003 domain](#) on page 118

Overview

Introduction

The Configuration Wizard enables you to configure the Avaya CallPilot server software. You can rerun the Configuration Wizard to update or review the server configuration.

The Configuration Wizard is accessible from CallPilot Manager (a web-based user interface). This chapter describes how to:

- log on to the operating system on the CallPilot server
- log on to the CallPilot server with CallPilot Manager run the Configuration Wizard

- change the pcAnywhere caller passwords or set the Remote Desktop Policy
- configure CallPilot to operate in a Windows 2000 or 2003 domain

 **Caution:**

Risk of improper configuration

You must use the Configuration Wizard to change the computer name. If you use the operating system method to change the computer name, it is not properly updated in the CallPilot software.

Plan your responses to the Configuration Wizard

Ensure you have planned your responses to the Configuration Wizard by completing the "Configuration Wizard worksheet" in the CallPilot Installation and Configuration Task List.

Online Help for the Configuration Wizard

Each page in the Configuration Wizard contains a Help button and provides detailed instructions regarding the selection or data entry required. Click Help at any time to get additional instructions.

Running the Configuration Wizard to detect replacement boards

When you replace MPB boards or MPC-8 cards, you must rerun the Configuration Wizard to detect and initialize the hardware. You do not need to change any data in the Configuration Wizard to perform this operation, but you do need to apply the configuration changes as instructed on the last page of the Configuration Wizard.

Logging on to Windows 2003 on the CallPilot server

Introduction

If you want to access CallPilot Manager from the web browser embedded on the CallPilot server, you must first log on to Windows 2003 on the CallPilot server. Alternatively, you can access CallPilot Manager from any PC that has network access to the CallPilot server.



Important:

When logging on, ensure that the CAPS key is not on. The password is case-sensitive.



Important:

When the system starts up, a mini-setup process launches which consists of a number of restarts. When this process is completed, the Windows Logon screen appears

To log on to Windows 2003 on the CallPilot server

1. Ensure that the CallPilot server has started and the operating system logon dialog box appears.
2. Type the user ID and password.

User ID	Administrator	You can choose to log on with a different user ID that has local administrative privileges.
Password (default)	Bww250 (or current Administrator password if it has been changed)	Passwords for operating system accounts should be changed from default values to strong values known only to the customer. CallPilot security is ultimately only as good as the passwords used.

3. Click OK.
4. Continue with [Running the Setup Wizard](#) on page 106.

Running the Setup Wizard

After you type the user ID and password, the CallPilot Setup Wizard welcome screen appears.

 **Note:**

For more information on the Setup Wizard, see the *Upgrade and Platform Migration Guide* (NTP NN44200-400).

To run the Setup Wizard

1. Read the information displayed on the screen and click Next.

Result: The Need SU/PEP Installation? screen appears.

2. If there are Service Updates (SUs) or PEPs available, you can choose to install them now. Select Yes or No and click Next.

If you choose Yes, install SU/PEPs:

Result: The Installing SU/PEP screen appears.

Install all the required SUs and PEPs.

 **Note:**

Restart your computer (if required) after all SUs and PEPs are installed.

Click Next to continue if no restart is required. Otherwise, restart the Wizard.

If you choose No, do not install SU/PEPs now.

Result: The Platform Validity Check screen appears.

3. View the items on the validity check and click Next.
4. When the system asks you if you have data to restore, select No.
5. Click Next to complete the Setup Wizard.
Result: The Finished screen appears.
6. Read the information displayed on the Finished screen and click Finish.
7. Continue with [Logging on to the CallPilot server with CallPilot Manager](#) on page 107.

Logging on to the CallPilot server with CallPilot Manager

Introduction

The Configuration Wizard is a menu item in CallPilot Manager. CallPilot Manager is the web-based CallPilot management tool, and can be accessed from any PC that has network access to the CallPilot server.

You can also access CallPilot Manager from the web browser on the CallPilot server. This may be the simplest method when installing CallPilot for the first time.

Logon process overview

The process for logging on to the CallPilot server with CallPilot Manager is the same for remote or local CallPilot servers. The logon process is completed in two stages:

1. Launch the web browser (on the CallPilot server, or on any PC that has network access to the CallPilot server), and then connect to CallPilot Manager.

For new installations, CallPilot Manager is located on the CallPilot server. The URL syntax is `http://CallPilot server host name or IP address/cpmgr/`

Example: `http://sunbird/cpmgr/`, where sunbird is the host name.

If you installed CallPilot Manager on a stand-alone web server (a separate PC that functions as a web server for CallPilot), the URL syntax is `http://web server host name or IP address/cpmgr/`



Note:

For more details, see [Relationship of the CallPilot Manager web server to the CallPilot server](#) on page 108.

2. Log on to the CallPilot server with an administrator's mailbox number and password.

Relationship of the CallPilot Manager web server to the CallPilot server

Example

The CallPilot Manager web server software can be installed on the CallPilot server or on a stand-alone server. If the CallPilot Manager web server software is installed on a stand-alone server, you must know the CallPilot Manager server's host name or IP address, as well as the CallPilot server's host name or IP address.

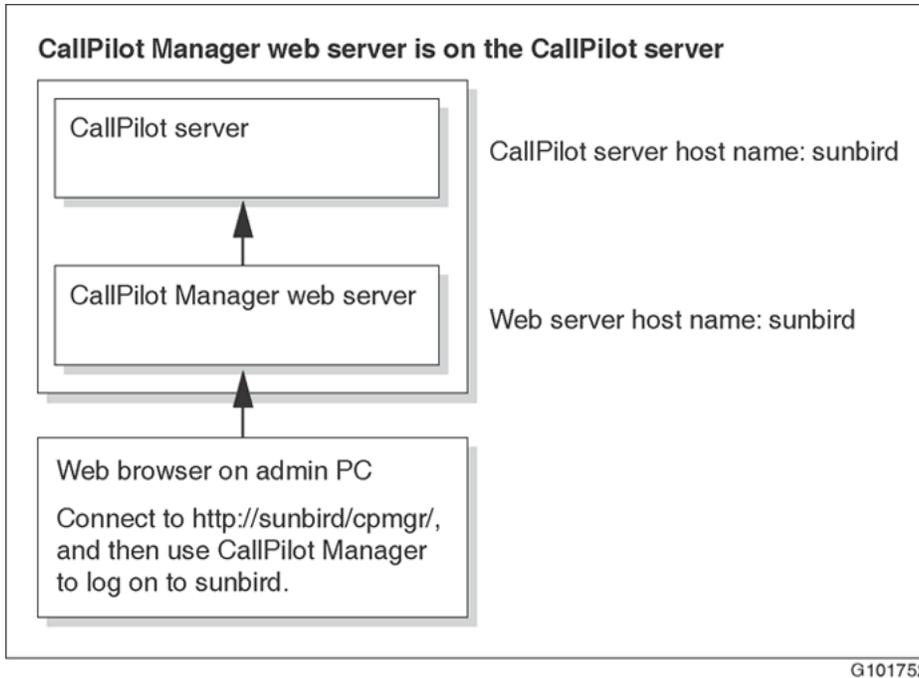


Figure 27: CallPilot Manager on CallPilot server

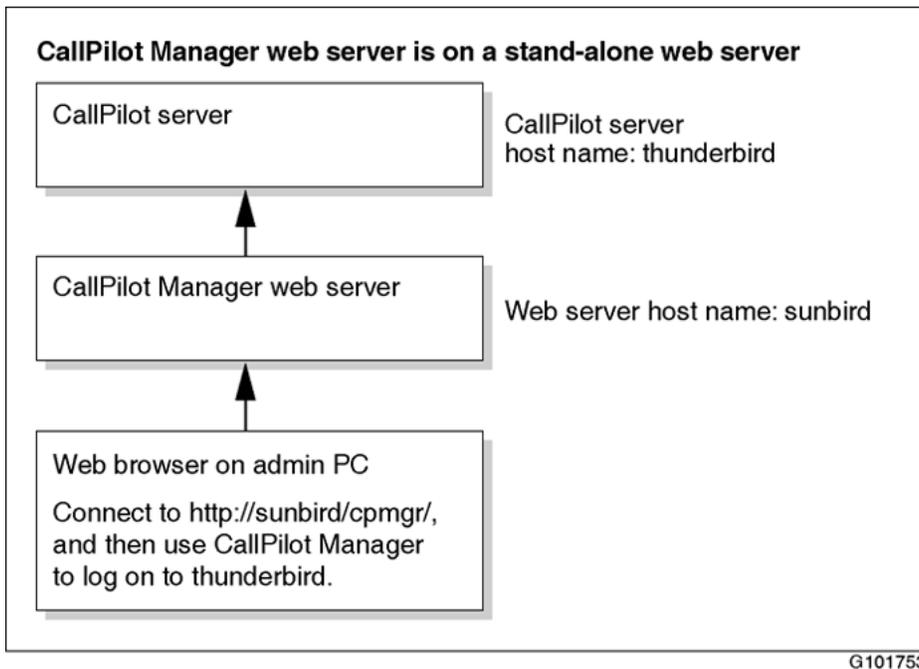


Figure 28: CallPilot Manager on stand alone server

To log on to the CallPilot server

1. Launch the web browser on your PC or on the CallPilot server.

If you are launching the web browser on	THEN
the CallPilot server	the CallPilot Manager, Login page appears automatically. Continue with step 2.
your PC	type the CallPilot Manager web server's URL in the Address or Location box of your web browser, and then press Enter. Example: http://sunbird/cpmgr/ When the connection is established, the CallPilot Manager - Login page appears. Continue with step 2.

 **Note:**

The URL automatically appears as http://<host name or IP address>/cpmgr/login.asp. On the CallPilot server, the URL is http://localhost/cpmgr/login.asp.

2. Type the administration mailbox number and password. The administrator mailbox number is 000000. The default password is 124578.
3. Do one of the following:
 - Type a server or location by one of the following methods:
 - choosing the list of pre-configured servers or locations in the Preset server list box
 - choosing the Last Server Accessed item
 - typing the address manually
 - Type the CallPilot server host name or IP address in the Server box.

 **Note:**

If you are logging on to the CallPilot server from a PC, type the actual CallPilot server name or IP address in the Server box. If you type local host instead of the CallPilot server name or IP address, you cannot establish an Application Builder connection to the CallPilot server from CallPilot Manager or make calls to the phoneset to play or record greetings.

If the CallPilot server that you are connecting to has Network Message Service (NMS) installed, type the CallPilot server host name or IP address in the Server box, and then type the name of the switch location on which the administration mailbox resides in the Location box.

4. Click Login.

Result: The main CallPilot Manager page appears.

**Note:**

Logging on for the first time forces you to change the password using numeric characters. (This is not a strong password, as described in the CallPilot Fundamentals Guide.)

5. Continue with [Running the Configuration Wizard](#) on page 111.

Running the Configuration Wizard

Introduction

This section describes how to access and run the Configuration Wizard.

Requirements

- CallPilot language CD, if you are installing, adding, or upgrading languages
- completed "Configuration Wizard worksheet" from the CallPilot Installation and Configuration Task List
- CallPilot keycode and dongle ID (serial number)

To run the Configuration Wizard

1.  **Important:**

For each page in the Configuration Wizard, follow the instructions on the page. Use the information you recorded in the "Configuration Wizard worksheet" in the CallPilot Installation and Configuration Task List.

If you have upgraded your CS 1000S to a CS1000E, the Terminal Numbers (TNs) on the CS 1000 were remapped to the large system format. For CallPilot to operate, you must change the switch type to M1 and the TNs to the large system format in the Configuration Wizard Switch Information page.

If you need additional instructions, click Help. If you are rerunning the Configuration Wizard, some pages may be prefilled. Some pages also contain default values. If the prefilled information does not match the information planned for this server, then update any prefilled values as required.

Log on to CallPilot Manager. See [Logging on to the CallPilot server with CallPilot Manager](#) on page 107.

2. Click the Configuration Wizard shortcut on the main CallPilot Manager page, or select Tools -> Configuration Wizard.

Result: The Welcome page of the Configuration Wizard appears.

3. Click Next to go to the next page.
4. Read the instructions carefully on each page. Click Help on the Configuration Wizard page if you need additional instructions. When you are finished with a page, click Next to continue.

 **Note:**

If you would like to change the CallPilot administrator account password while the CallPilot server is in a domain, follow the below steps:

- a. Log on with one of the CallPilot local accounts.
 - b. Right-click on My Computer and select Properties.
 - c. Select Computer Name.
 - d. Click Change and select Workgroup.
 - e. Type WORKGROUP as the workgroup name.
 - f. Restart and log on with one of the CallPilot local accounts.
 - g. Run the Configuration Wizard to change the CallPilot administrator password or the CallPilot server host name.
5. When you reach the end of the Configuration Wizard, click Finish to save the Configuration Wizard changes, or click Cancel to discard any changes. No changes are implemented unless you click Finish.

Result: The Configuration Wizard requires up to an hour to apply changes, depending on the number of languages you are installing or updating, and the size of the system. When CallPilot completes the configuration changes, you are prompted to restart the server.

6. Restart the server.

 **Note:**

Ensure you use the restart procedure documented in the CallPilot Installation and Configuration Task List.

Result: The server restarts and the configuration changes are in effect.

 **Note:**

If you run the Configuration Wizard after your CallPilot server is added to a domain, two procedures do not work until you remove the server from the domain. The two procedures are: changing the computer name, and changing the local administrator account. For more information, see [Configuring CallPilot to operate in a Windows 2000 or 2003 domain](#) on page 118.

Considerations on configuring STI links for the CallPilot tower and rackmount servers

The Configuration Wizard application is used to configure the switch telephony interface (STI) links and the DS0 channels between the MGate cards in the Meridian 1 Meridian 1 switch and the MPB16-4 or MPB96 boards in the CallPilot server. Each MPB16-4 board can have two STI links and each STI link can have a maximum of 32 DS0 channels. Each MPB96 board can have three STI links. Refer to the Configuration Wizard online help for more information on configuring the STI links and the DS0 channels.

 **Note:**

Each STI link must be programmed individually with the matching MGate card on all 32 channels.

If your CallPilot server contains one MPB96 board, you must completely program the first STI link before moving on to the next STI link of that board.

If your CallPilot server contains three MPB96 boards, you must start populating data on the first MPB96 board and completely program the first STI link before moving on to the next STI link of that board. Once all 3 STI links of the first MPB96 board are completely populated, you may then move on to the second MPB96 board.

If your CallPilot server contains two MPB16-4 boards connected to two MGate cards and you need more than 32 DS0 channels between the CallPilot server and the switch, then you must configure both STI links on MPB16-4 #1 before starting to configure the STI links on MPB16-4 #2. Start configuring the STI links on MPB16-4 #2 only when you need more than 64 DS0 channels. Make sure that you are always able to identify the MPB16-4 boards.

Make sure that you are always able to identify the MPB16-4 boards. See [Identifying the location of MPB 1 and MPB 2](#) on page 56 for the numbers of the slots in which the MPB #1 and MPB #2 can be installed on CallPilot servers.

If you configure an STI link on MPB16-4 #2 before configuring both STI links on MPB16-4 #1, the DS0 channels on MPB16-4 #2 are not functional. As a result, you experience no voice in the slot that holds the MPB16-4 #2 board.

What is next?

Your next step will depend on your choice of a remote support tool.

- If you are using pcAnywhere, continue to [Changing pcAnywhere caller passwords](#) on page 114.
 - If you are using Remote Desktop Connection, continue to [Setting Remote Desktop Policy on a Server](#) on page 115.
-

Changing pcAnywhere caller passwords

Introduction

With pcAnywhere, you can perform advanced administrative tasks on the server from a remote PC. You can control the server as though you were directly connected to the server.

pcAnywhere is installed and configured on the server at the factory. One licensed copy of pcAnywhere is provided for the server on the CallPilot Application CD-ROM.

To install pcAnywhere on another PC, you must purchase a separate license. For instructions on how to install and configure pcAnywhere on another PC, see the *CallPilot Administrator's Guide*(NN44200-601).

To change pcAnywhere caller passwords

1. Stop the pcAnywhere session, if one is running.
2. Click Start -> Programs -> Symantec pcAnywhere.
Result: The Symantec pcAnywhere window opens.
3. Click the Hosts icon in the pcAnywhere section of the Symantec pcAnywhere window.
Result: The list of hosts is displayed.
4. Right-click the CallPilot Support icon, and then choose Properties from the pop-up menu.
Result: The Host Properties: CallPilot Support dialog box appears.
5. Click the Callers tab.
6. Right-click the CallPilotDist icon, and then choose Properties from the pop-up menu.

7. In the Password box, type a new CallPilotDist password.
8. In the Confirm Password box, type the CallPilotDist password again.
9. Click Apply.
10. Click OK.
11. Click OK to return to the main Symantec pcAnywhere window.
12. Double-click the CallPilot icon to restart the pcAnywhere session.

What is Next?

Continue to [Configuring CallPilot to operate in a Windows 2000 or 2003 domain](#) on page 118.

Setting Remote Desktop Policy on a Server

CallPilot server comes with the Remote Desktop server enabled and configured for use by default. If necessary, remote desktop access can be enabled or disabled as follows:

To set remote desktop policy

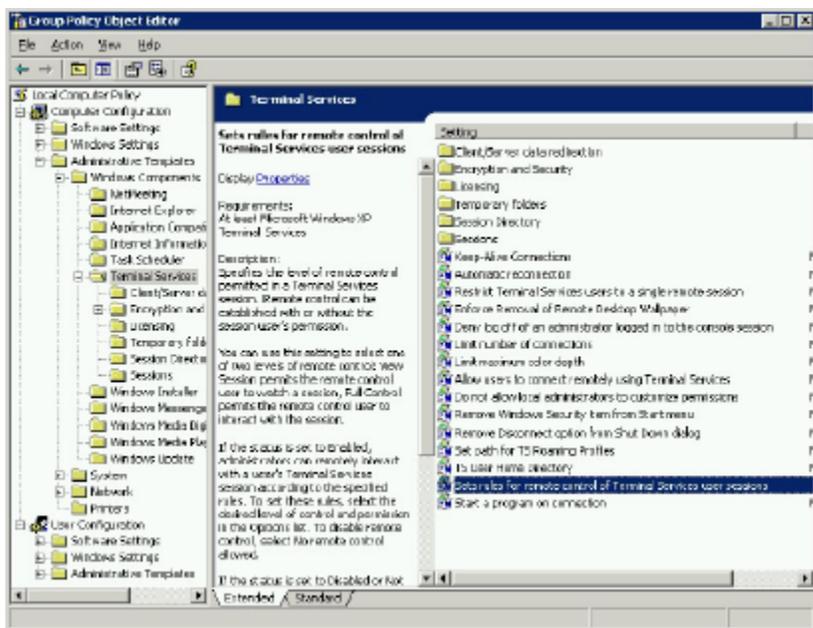
1. From the CallPilot server desktop, right-click My Computer, then choose Properties, and click on the Remote tab.

Result: The System Properties screen appears.

Configuring the Avaya CallPilot® server software



2. Ensure the Allow users to connect remotely to this computer option is selected. Click OK to close the window.
3. Open the Group Policy Snap-in to choose from the five options available for remote control settings. Open a command prompt window by clicking Start > Run.
Result: The Open window appears.
4. Type gpedit.msc and click OK or press Enter.
Result: The Group Policy Object Editor window appears.



5. On the left side of the window, expand Computer Configuration, Administrative Templates, Windows Components, and then select Terminal Services.
6. On the right side of the window, double-click Sets Rules for Remote Control Terminal Services User Sessions.
7. The Sets Rules for Remote Control Terminal Services User Sessions window appears.
8. Select Enabled to load options into the box.
9. The default and recommended setting for CallPilot is Enabled with Full Control without User's Permission selected. This setting allows for RDC sessions without requiring interaction or consent from a local console user.

Adjust the settings as required, and click OK to close the screen.
10. Click File > Close to close the Group Policy Object Editor.

 **Note:**

For instructions on installing and configuring Remote Desktop Connection (RDC), see the *CallPilot Troubleshooting Reference Guide* (NN44200-700).

What is Next?

Continue to [Configuring CallPilot to operate in a Windows 2000 or 2003 domain](#) on page 118.

Configuring CallPilot to operate in a Windows 2000 or 2003 domain

Introduction

Avaya supports CallPilot as a member in a Windows 2000 or 2003 domain. Customers can add their server machine to a Windows 2000 or 2003 domain for added security and manageability. Whether you are upgrading to CallPilot 4.0 or installing a new CallPilot 4.0 system, you can move your server from a Windows workgroup to a Windows 2000 or 2003 domain.



Note:

You do not need to add CallPilot to a domain. This procedure is optional. Avaya will continue to support CallPilot 4.0 in a workgroup. If you do not want to add your server to a domain, continue with [Testing the Avaya CallPilot® installation](#) on page 129.

To add your CallPilot server to a domain, you require network administrator privileges. To perform this procedure, you can either work with your network administrator, or ask your network administrator to create a user account with network administrator privileges.

When you add your CallPilot server to a domain, Avaya recommends that you see the latest Distributor Technical Reference (DTR), available on the web site .

This section describes how to:

- set domain group policy
- add your CallPilot server to the domain
- stop and disable Win32 Time Service on the CallPilot server
- set up user accounts for remote access
- run Configuration Wizard in a domain

To set domain group policy

When you install Release 4.0 of CallPilot, the installation creates local accounts that contain default strong passwords of six characters. As a result, your local domain group policy can conflict with these default settings. The CallPilot administrator account can be affected. See

[Running the Configuration Wizard](#) on page 111 for information on how to change the user account.

If you identify conflicts, you can adjust your group policies for CallPilot, or you can exclude the CallPilot server machine from a specific group policy.

When you add your CallPilot server to a domain, you must also consider that the Windows 2003 Domain Controller determines the security policy that applies to the server.

 **Note:**

Avaya strongly recommends that you add the server to a domain after running the Configuration Wizard.

To add CallPilot server to a domain

After you install and configure your CallPilot server, and you confirm that your network administrator has set up a Domain Controller and a DNS server on the network, you can add your server as a member of an existing domain.

To add the server as a member of an existing domain:

1. On the CallPilot server, courtesy stop all CallPilot channels. See the *Installation and Configuration Task List Guide* (NN44200-306), for more information.
2. Compare the M1/Succession time to the time on the Domain Controller, or the time on any existing Domain member computer.

 **Note:**

Avaya recommends that the difference between the M1/Succession time and the Domain Controller time does not exceed 10 seconds.

 **Note:**

The CallPilot server time is updated by the M1/Succession time, so when you change the M1/Succession time, the CallPilot server time is also updated.

- a. If the difference in the M1/Succession time and the Domain Controller time is greater than 10 seconds, go to Step 3 to change the M1/Succession time to match the Domain Controller time.
 - b. If the difference in the M1/Succession time and the Domain Controller time is less than 10 seconds, go to Step 4. You do not need to adjust the time.
3. To change M1/Succession time to match the Domain controller time, perform the following steps:
 - a. Log on to the M1/Succession server and go to LD 2.

- b. Type TTAD and press Return.

Result: The current M1/Succession format for the time and the time appear. An example is:

<day> <month> <year> <hour> <minute> <sec> 12 01 2005 22 35 00

- c. Type STAD and press Return.

Result: The time and date appear. An example is:

<day> <month> <year> <hour> <minute> <sec> 12 01 2005 22 35 00

- d. Change the time to match the Domain Controller time.

 **Note:**

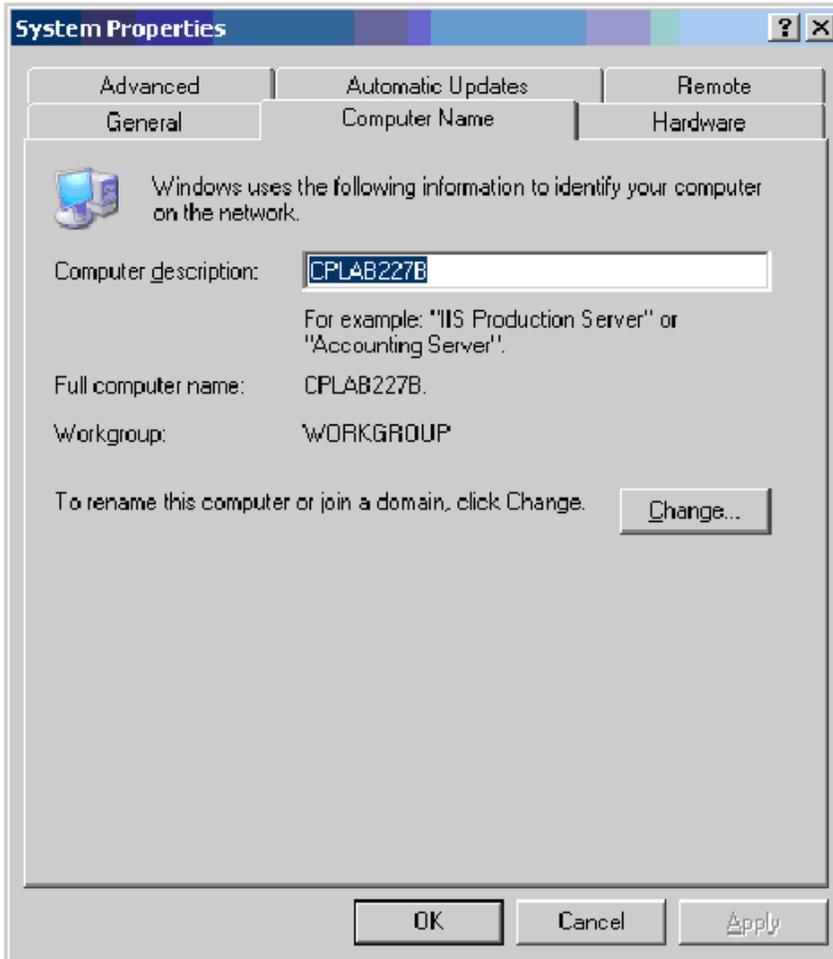
Avaya recommends that you keep the time difference between the M1 and the Domain Controller time to within a few seconds (+/- 10 seconds). The maximum difference can be up to five minutes before Kerberos authentication problems can arise. Once a month, check the times on the M1/Succession and the domain to ensure that the five minute tolerance is not exceeded. If the time difference is exceeded by five minutes, you can experience problems with Event Viewer, audit logs, and local system network shares. You can also receive messages on the local server that indicate that the CallPilot server time is out of synchronization with the Domain Controller. Day-to-day operation of the CallPilot server, however, should not be affected.

 **Note:**

For normal CallPilot operation, support, and maintenance, you must create a domain user account. In order for you to receive administrator privileges on the local server, the CallPilot administrator must add the domain user account to the CallPilot local administrator group.

4. Exit the pcAnywhere session if it is running.
5. On the CallPilot server Windows desktop, right-click on My Computer, and then select Properties.
6. In the System Properties window, click the Computer Name tab.

Result: The following System Properties window appears.



7. Click Change.

Result: The Computer Name Changes window appears.



8. To add the server to an existing domain, click the Domain option button in the Member of pane, and then type the name of the domain.
9. Click OK.

Result: The Domain Username And Password window appears.



10. Type the username and password from the user account on the Domain Controller that has remote access privileges.

 **Note:**

You need a domain administrator username and password.

11. Click OK.

Result: When the system processes your change successfully, the following dialog box appears, notifying you that the server now belongs to the specified domain.



12. Click OK.
13. Click Yes to restart your computer.

To stop and disable the Win32 Time Service

Note:

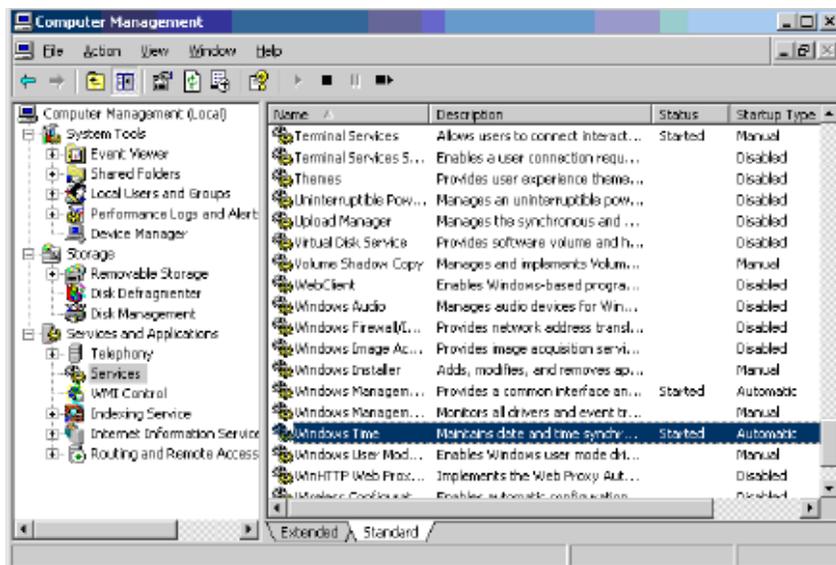
If you are on a T1/SMDI switch, this procedure does not apply to a T1/SMDI system.

To prevent the Domain Controller from controlling the CallPilot server time, you must disable the Win32 time Service on the CallPilot server. This allows the M1 or Succession switch to continue to control the CallPilot server time.

To stop and disable the Win 32 Time Service

1. Log on to the CallPilot server.
2. Right-click on My Computer and select Manage > Services and Applications > Services.

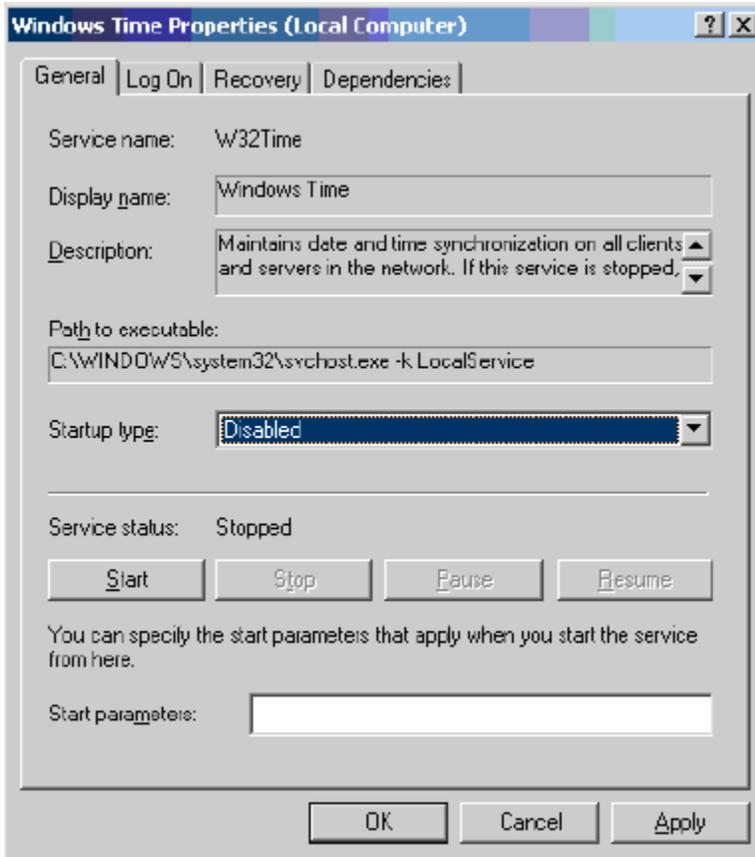
Result: The Computer Management window appears:



- a. In the right pane, right-click on Windows Time and select Stop.

- b. When the Service stops, right-click on Windows Time and select Properties > General tab.

Result: The Windows Time Properties (Local Computer) window appears:



- c. Select Disabled from the Startup type menu.
- d. Click Apply, and then click OK.
- e. On the Computer Management window, verify that the Windows Time service is disabled.
- f. Close the Computer Management window.

To set up user accounts for remote access domain

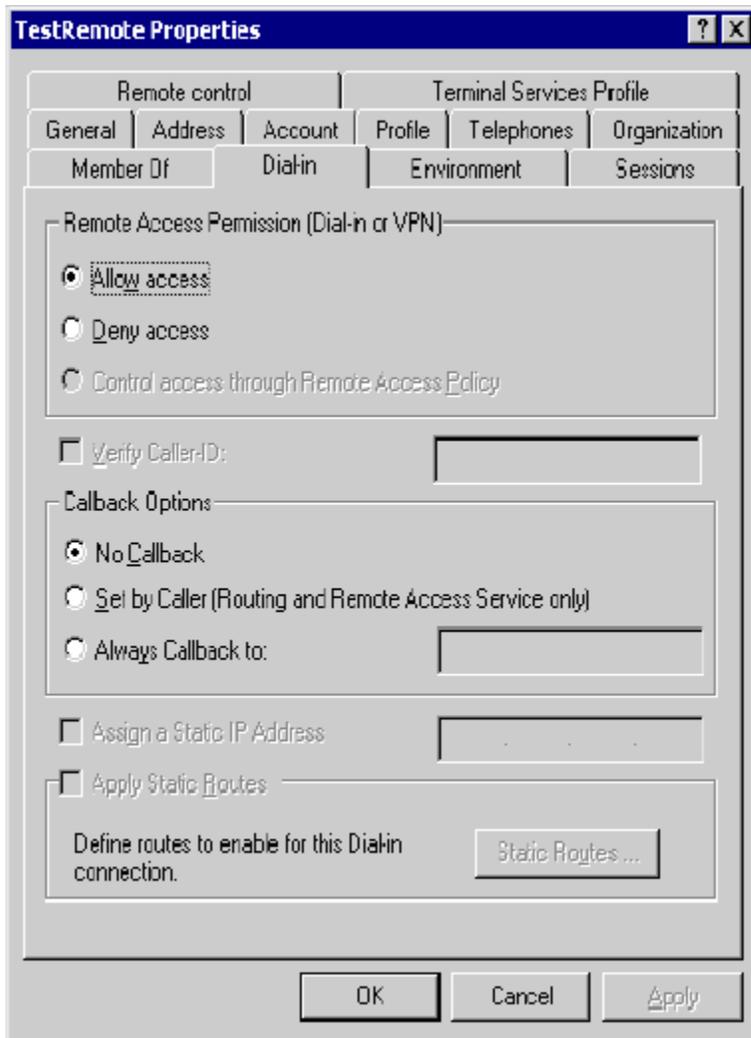
In a Windows Server 2003 domain environment, you must create a dial-up user as a Domain user on the Domain Controller and assign dial-in access permissions to this user. When dialing in to the RAS configuration CallPilot Release 4.0 server, the Domain controller authenticates the username and password.

*** Note:**

Local dial-in access is no longer available for the administrator account through Routing and Remote Access server (RRAS). You can obtain remote dial-in access to the CallPilot system by setting up a domain account with dial-in permissions.

After you set up a domain user account and assign dial-in access permission, you have two options to log on to the local CallPilot system using dial-in access permission.

See below an example of a Domain user account with dial-in access:



Option 1: Use the local Administrator account for remote logon.

To perform Option 1, follow the steps below:

1. Ask the network administrator for a user account allowing dial-in access permission.

 **Note:**

Ask the network administrator for a username and password that is different from the username and password for your local CallPilot Administrator account. Record the username and password carefully as it will be required for remote support of the CallPilot server.

2. When you dial in to the server, you are prompted for a dial-in Domain user account and password. Type the username and password that you received in Step 1.
3. Initiate a pcAnywhere or a Remote Desktop Client (RDC) session.
4. Type the local CallPilot administrator account to log on to the CallPilot server.

 **Note:**

Since there is no local record for the Domain user account, two user accounts must be maintained: the Domain user account, and the local account.

Option 2: Use the Domain user account for remote logon

To perform Option 2, follow the steps below:

1. Ask the network administrator for a user account allowing dial-in access permission.

 **Note:**

Ask the network administrator for a username and password that is different from the username and password for your local CallPilot Administrator account. Record the username and password carefully as it will be required for remote support of the CallPilot server. The dial-in account must be added to the CallPilot local Administrator group to grant administrator privileges to support personnel.

2. Initiate a pcAnywhere or a RDC session.
3. When you dial in to the server, the system prompts you for a dial-in domain user account and password. Type the username and password that you received in Step 1.



Note:

This option manages the user account in one location, for both dial-in access through pcAnywhere or RDC.

To run Configuration Wizard in a domain

After you add the CallPilot server to a domain, the domain account that is used to log on to the CallPilot server does not have network administrator privileges. As a result, if you run the Configuration Wizard after you add your CallPilot server to the domain, two procedures do not work until you remove the server from the domain. The two procedures are: changing the computer name, and changing the local administrator account. To perform these two procedures when your server is in a domain, you must remove the server from the domain, perform the procedure, and then add the server to the domain again.

To change the computer name

To change the computer name when you run Configuration Wizard and CallPilot is a member of a domain, perform the following steps:

1. Ask your network administrator to remove the CallPilot server from the domain and add the server to a workgroup. You can also perform this step on your own, if you acquire network administrator privileges from your network administrator.
2. Shut down and restart the CallPilot system.
3. Run the Configuration Wizard and select the option to change the computer name.
4. Shutdown and restart the CallPilot system.
5. Ask your network administrator to add the CallPilot server to the domain. You can also perform this step on your own, if you acquire network administrator privileges from your network administrator.
6. Shutdown and restart the CallPilot system.

To change the local account passwords

To change the local account passwords when you run Configuration Wizard and CallPilot is a member of a domain, perform the following steps:

1. Ask your network administrator to remove the CallPilot server from the domain and add the server to a workgroup. You can also perform this step on your own, if you acquire network administrator privileges from your network administrator.
2. Shut down and restart the CallPilot system.
3. Run the Configuration Wizard and select the option to change the account passwords.
4. Shutdown and restart the CallPilot system.
5. Ask your network administrator to add the CallPilot server to the domain. You can also perform this step on your own, if you acquire network administrator privileges from your network administrator.
6. Shutdown and restart the CallPilot system.

What is next?

Continue with [Testing the Avaya CallPilot® installation](#) on page 129.

Chapter 6: Testing the Avaya CallPilot® installation

In this chapter

[Checking that Avaya CallPilot is ready to accept calls](#) on page 129

[Testing the connection to the ELAN subnet](#) on page 133

[Testing the connection to the NNS Subnet](#) on page 134

[Verifying that CallPilot can receive calls](#) on page 135

[Testing the CallPilot software and channels](#) on page 136

Checking that Avaya CallPilot is ready to accept calls

Important:

CallPilot is not ready to accept calls until the CallPilot services are fully operational. CallPilot services require approximately 10 minutes after starting up the CallPilot server to become fully operational.

Introduction

CallPilot uses various system-ready indicators to indicate when it is ready to accept calls, including:

- displaying messages in dialog boxes on the CallPilot server monitor after logon. It also displays a status icon in the top right corner of the CallPilot Manager window.
- generating events that can be viewed in the Event Browser or Alarm Monitor in CallPilot Manager
- displaying status using the hex display (applies only to the 201i or 202i server)

The system-ready indicators described in this section appear when you restart the server, and also when CallPilot is running if a change in system readiness status occurs.

The system-ready indicators appear only if the Configuration Wizard has previously been run on the server. The CallPilot server is not ready to accept calls if the Configuration Wizard has not been run.

 **Note:**

It is possible that the Configuration Wizard was run at the factory or channel partner's site before it was shipped to the customer site. If this is the case, then system-ready indicators are visible when the CallPilot server is started the for first time at the customer site.

Checking system readiness by observing the dialog box messages

A system-ready indicator dialog box appears on the screen any time there is a change in system readiness status. You can close these dialog boxes at any time. If the status changes, a dialog box appears again.

At all times, a system-ready indicator icon appears in the task bar in the bottom right corner of the screen. To view the system-ready indicator dialog box after you close it, double-click the system-ready indicator icon. To view the current status (boot, pass, warn, or fail), place the mouse pointer over the system-ready indicator icon. Help text (roll-over text), which states the current status, appears after a few seconds.

Immediately after you log on to the server, the dialog box, shown in [Figure 29: SRI CallPilot boot fail](#) on page 130, appears on the screen if CallPilot services are not yet fully operational. It can take approximately 1 minute after logon for the dialog box to appear.

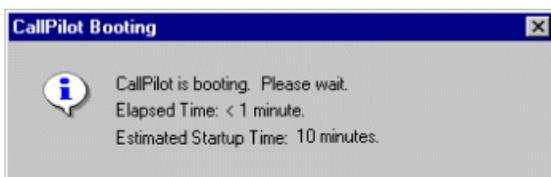


Figure 29: SRI CallPilot boot fail

The Elapsed Time indicates how much time has passed since the CallPilot application began its boot sequence.

 **Note:**

This dialog box may not appear if enough time has passed between starting up the CallPilot server and logging on for CallPilot services to become fully operational. It takes approximately 10 minutes after starting up the CallPilot server for CallPilot services to become fully operational.

If the CallPilot start sequence is passed successfully (that is, CallPilot services are fully operational), the dialog box, shown in [Figure 30: SRI CallPilot boot pass](#) on page 131, appears.



Figure 30: SRI CallPilot boot pass

Click OK to close the dialog box.

If there are errors, one of the following two dialog boxes appears (depending on the severity of the problem).



Figure 31: SRI CallPilot warning

Close the dialog box by clicking the X in the upper right corner. Check the Event Browser or Alarm Monitor in CallPilot Manager for more details. For instructions, see the CallPilot Manager online Help.

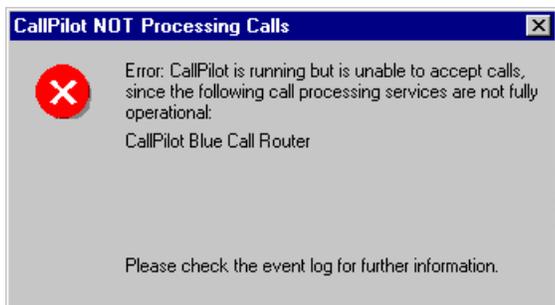


Figure 32: SRI CallPilot error message

Close the dialog box by clicking the X in the upper right corner. Check the Event Browser or Alarm Monitor in CallPilot Manager for more details. For instructions, see the CallPilot Manager online Help.

Alternative methods for verifying that CallPilot is ready to accept calls

View events in CallPilot Manager or in the operating system Event Viewer on the server

The Pass, Warning, and Error system-ready indicator messages appear as events in the Event Browser and Alarm Monitor in CallPilot Manager, and in the operating system Event Viewer on the server.

By default

- the Event Browser and Alarm Monitor show only the latest 100 events

Change the default settings to remove the system-ready indicator events from the Event Browser and Alarm Monitor windows.

- the Event Browser lists only Critical events

You can change the Filter Criteria so that Major, Minor, and Information events are listed as well.

For detailed instructions on viewing events, see the CallPilot Manager online Help.

Observe the HEX display (for the 201i or 202i server only)

The HEX display on the 201i or 202i server faceplate displays the following messages.

 **Note:**

The DOWN, OK, MIN, MAJ, CRI, and "???" messages can appear regardless of whether the Configuration Wizard has been run. Some MIN, MAJ, and CRI events may appear because the server has not been configured. These events may be resolved after running the Configuration Wizard. The BOOT, PASS, WARN, and FAIL messages are system-ready indicator messages; they do not appear if the Configuration Wizard has not been run.

IPE CallPilot server HEX display	Description
DOWN	The operating system is starting.

IPE CallPilot server HEX display	Description
OK	The operating system start sequence has passed.
BOOT	CallPilot is starting and is not yet fully operational. Please wait.
PASS	CallPilot is fully operational and ready to accept calls.
WARN	CallPilot is ready to accept calls; however, some services failed the start sequence. Check the event log for further information.
FAIL	CallPilot failed the start sequence and cannot accept calls. Check the event log for further information.
MIN	A minor alarm has occurred. Check the event log for further information.
MAJ	A major alarm has occurred. Check the event log for further information.
CRI	A critical alarm has occurred. Check the event log for further information.
???	An alarm of unknown severity has occurred. This error should not occur on a properly installed system. The severity of this event is treated as higher-than-critical.

Testing the connection to the ELAN subnet

Introduction

This procedure tests the network connection between the server and the CS 1000 system over the ELAN subnet.



Important:

Disconnect the Avaya Server Subnet (NS Subnet) from the ELAN subnet before testing to ensure that the ping is testing only the ELAN subnet.

To test the connection to the ELAN subnet

1. Click Start -> Programs -> Accessories -> Command Prompt.

Result: The Command Prompt window appears.

2. Type ping followed by the ELAN subnet IP address for the CS 1000 system, and then press Enter.



Note:

This is the ELAN subnet IP address specified for the CS 1000 system in. See the Configuration Wizard worksheets that you completed in the CallPilot Installation and Configuration Task List for the IP address.

Example: ping 255.255.255.255

Result: The display should indicate a successful ping. If the ping is not successful, check the connection from the CallPilot server's ELAN subnet card to the CS 1000 system.

3. If the CallPilot server is also connected to a Avaya Server Subnet (NS Subnet), then continue with "Testing the connection to the NNS Subnet" on page 160.

If the CallPilot server is not connected to a Avaya Server Subnet (NS Subnet), then type exit and press Enter to close the Command Prompt window. Then continue with [Verifying that CallPilot can receive calls](#) on page 135.

Testing the connection to the NNS Subnet

Introduction

This procedure tests the network connection between the server and the Avaya Server Subnet (NS Subnet). This applies only if CallPilot has an NNS Subnet card and is connected to an NNS Subnet.



Important:

Disconnect the NNS Subnet from the ELAN subnet before testing to ensure that the ping is testing only the NNS Subnet.

To test the connection to the NNS Subnet

1. Click Start -> Programs -> Accessories -> Command Prompt.

Result: The Command Prompt window appears.

2. Type ping followed by the NNS Subnet IP address of another PC on the NNS Subnet, and then press Enter.

Example: ping 255.255.255.255

Result: The display indicates a successful ping.

3. Type exit, and then press Enter to close the Command Prompt window.

Verifying that CallPilot can receive calls

Introduction

The following procedure is a basic test to verify that CallPilot is able to receive calls from the CS 1000 system and answer those calls. A more thorough test that requires the use of CallPilot Manager is described in [Testing the CallPilot software and channels](#) on page 136.

To verify that CallPilot can receive calls

1. Ensure that CallPilot services are fully operational before you begin.
For instructions, see [Checking that Avaya CallPilot is ready to accept calls](#) on page 129.
2. Dial the main Voice Messaging DN that you defined in the Configuration Wizard.
3. Listen for a response from CallPilot (for example, "CallPilot from Avaya ..."), and then hang up.

If you do not get a response, then do the following:

- a. Check the cabling between the server and the CS 1000 system.
- b. Verify that the CS 1000 system is processing calls to other extensions.
- c. see the CallPilot Server Maintenance and Diagnostics guide for your server.

What is next?

Continue with [Testing the CallPilot software and channels](#) on page 136.

Testing the CallPilot software and channels

Introduction

This section provides a series of tests of the CallPilot installation, including verifying that

- you can leave a message
- you can retrieve a message
- each call channel and multimedia (DSP) channel is functioning properly

Before you begin

- Ensure that you have configured the CS 1000 system and CallPilot server, as described in this guide.
- Obtain the ACD DN for CallPilot.
- Identify a phoneset DN that exists on the CS 1000 system that you can use for testing.
- Have a pencil and paper ready to record the results of the tests.

To verify that you can leave a message

Complete the following procedures to perform this test:

1. [To add a user for testing purposes](#) on page 136
2. [To configure the Voice Messaging DN](#) on page 137
3. [To leave a message](#) on page 138

To add a user for testing purposes

1. Log on to the operating system on the CallPilot server.

For instructions, see [Logging on to Windows 2003 on the CallPilot server](#) on page 105.

 **Note:**

Although you can access CallPilot Manager from any PC that has network access to the CallPilot server, later tests require that you be logged on to the CallPilot server.

2. Log on to CallPilot Manager.

For instructions, see [Logging on to the CallPilot server with CallPilot Manager](#) on page 107.

3. Click Users. Add User.

Result: The Express Add page appears.

4. Type the required information.

Each required field is marked with an asterisk (*). Accept the default values for other fields.

For example, create a user named TEST USER.

 **Important:**

The tests in this section use the mailbox number 8050 as an example. Ensure that you specify a DN that is defined on the CS 1000 system.

5. Click Advanced User Add.

Result: The Advanced User Add page appears, and the information you have already entered appears.

6. Scroll down to the Security section of the page and specify a mailbox password.

Record the password. Leave all other fields at their default values.

7. Click Express Add.

Result: The Express Add page appears.

8. Click Add.

Result: CallPilot Manager displays a summary of the user just added.

To configure the Voice Messaging DN

 **Note:**

If you have already configured a Voice Messaging CDN in the Configuration Wizard, then you can skip this procedure. If you are not sure, continue with this procedure to verify that a Voice Messaging CDN is present, or to configure one if necessary.

1. Click System. Service Directory Number.

Result: The Service Directory Number page appears.

2. Click New.

Result: The SDN Detail page appears.

3. In the Service DN box, type the primary Voice Messaging DN for CallPilot.



Note:

If there are no voice channels installed on CallPilot, then use the Fax or Speech Recognition primary DN as the Voice Messaging DN for these tests. You can still use the Voice Messaging application as described in this procedure.

4. In the Application Name box, select Voice Messaging.
5. In the Media Type box, select Voice.



Note:

If there are no voice channels installed on CallPilot, then select Fax or Speech Recognition based on the DN that you specified in step 3.

6. Click Save.

To leave a message

1. From any active phoneset that is connected to the CS 1000 system, dial the Voice Messaging Service DN that you have just created.

Result: CallPilot plays the following prompt: CallPilot from Avaya. Mailbox?



Note:

If CallPilot does not answer the call or you do not hear a prompt, then check that the call channels and multimedia channels are in Idle state, as described in [Verifying that each call channel and multimedia channel is functioning properly](#) on page 140.

2. Type the mailbox number followed by number sign (#) (for example, 8050#).

Result: CallPilot plays the following prompt: Password?

3. Type the mailbox password 135246#.

Result: CallPilot plays the following prompt: The temporary password assigned by your administrator must be changed. To access your mailbox, please press 84 and change your password.

4. Press 84.

Result: CallPilot plays the following prompt: Password change. To authorize the change, please enter your old password followed by number sign.

5. Type 135246#.

Result: CallPilot plays the following prompt: Please enter your new password followed by number sign.

6. Type a new mailbox password followed by number sign (#) (for example, 805011#).
Result: CallPilot plays the following prompt: Please enter your new password again followed by number sign.
7. Type the new mailbox password again to confirm (for example, 805011#).
Result: CallPilot plays the following prompt: Your password has been changed. Your mailbox is empty.
8. Press 75 to compose a message.
Result: CallPilot plays the following prompt: Compose ...
9. Type the mailbox number, followed by number sign (#) twice (for example, 8050##).
Result: CallPilot plays the following prompt: To begin recording, Press 5. To end recording, press number sign.
10. Press 5 to record a message.
11. Record a message, and then press number sign (#) to stop.
Result: CallPilot plays the following prompt: Recording Stopped. There is a brief pause, followed by the prompt: To review the message, press 2, to send it, press 79...
12. Press 79 to send the message.
Result: CallPilot plays the following prompt: Message sent and deleted.
13. Press 83, and then hang up the phone.
14. Verify that the Message Waiting Indicator (MWI) is on.

To verify that you can retrieve a message

1. Pick up the telephone handset and dial the same Voice Messaging Service DN again.
2. When prompted, type the mailbox number where the message was left (for example, 8050#).
Result: CallPilot plays the following prompt: Password?
3. Type the mailbox password (for example, 805011#).
Result: CallPilot plays the following prompt: You have one new message. Message one. New. From ...

Important:

If you do not hear the exact message, You have one new message..., this indicates that the wrong prompts have been installed or that CallPilot did not install properly.

If you did not hear the correct message, contact your Avaya customer support representative.

4. Press 2 to play the message, and then listen to it.

5. Press 76 to delete the message.

Result: CallPilot plays the following prompt: Message 1 deleted.

 **Important:**

If you do not hear the exact message, Message 1 deleted, this indicates that the wrong prompts have been installed or that CallPilot did not install properly.

If you do not hear the correct message, contact your Avaya customer support representative.

6. Press 83 and then hang up the phone.

Verifying that each call channel and multimedia channel is functioning properly

These tests verify that the call channels and multimedia (DSP) channels are functioning properly.

The call channel is the channel that carries the call signal from the CS 1000 system to CallPilot. The multimedia channel is the CallPilot channel that processes the call and provides voice, fax, or speech recognition capability.

These tests consist of the following procedures:

- [To test call channels and voice channels](#) on page 141 (Skip this procedure if you do not have voice channels installed.)
- [To test call channels and fax channels](#) on page 142 (Skip this procedure if you do not have fax channels installed.)
- [To test call channels and speech recognition channels](#) on page 144 (Skip this procedure if you do not have speech recognition channels installed.)
- [To restore the SDN Table and put all channels back in service](#) on page 145

 **Note:**

These tests require that you access the Channel Monitor, Multimedia Monitor, and Service Directory Number pages in CallPilot Manager. If you need additional instructions for these CallPilot Manager pages, see the CallPilot Manager online Help, or to the *CallPilot Administrator's Guide* (NN44200-601). You must also access the System Monitor utility. The System Monitor utility is described in the chapter "Using CallPilot system utilities" in the *CallPilot Server Maintenance and Diagnostics guide* for your server.

To test call channels and voice channels

 **Note:**

If CallPilot has no voice channels, go to [To test call channels and fax channels](#) on page 142.
If CallPilot also has no fax channels, go to [To test call channels and speech recognition channels](#) on page 144.

1. In CallPilot Manager, click System -> Service Directory Number.

Result: The Service Directory Number page appears.

2. Ensure that the Voice Messaging Service DN is set to the ACD DN.

 **Note:**

If the Voice Messaging Service DN is not set to the ACD DN, then select the defined Service DN and click File / Properties. Make the required changes, and then click Save.

3. In the Application Name box, ensure that Voice Messaging is selected.
4. In the Media Type box, ensure that Voice is selected.
5. Click Maintenance / Multimedia Monitor.

Result: The Multimedia Monitor appears.

6. Select and start a maximum of eight voice channels for testing.

 **Note:**

Avaya recommends that you test a maximum of eight voice channels at one time. For example, if you have a 96-channel system, start only eight voice channels. When those eight voice channels are tested, stop them and start another set of voice channels.

7. Stop all fax and speech recognition channels, if these channels are present.
8. Verify that all voice channels are in Idle state.
9. In CallPilot Manager, click Maintenance / Channel Monitor.

Result: The Channel Monitor appears.

10. Select the whole system and stop all channels.
11. Select and start the same number of call channels as voice channels that you started.

Example: If you have started eight voice channels, then start eight call channels.

12. On the CallPilot server desktop, click Start -> Programs -> CallPilot -> System Utilities -> System Monitor.

Result: The CallPilot System Monitor window appears. By default, the Channel Monitor tab appears on top.

13. Observe the System Monitor window and verify that all the required multimedia (DSP) and call channels are in Idle state, and that all other channels are Off Duty (out of service).
14. Use a telephone to dial the service DN that you entered in the SDN table for Voice Messaging.
15. Verify that CallPilot answers the call and that the CallPilot greeting plays.
16. Observe the System Monitor and record which call channel and which voice channel change to Active states.
17. Hang up the telephone.
18. Repeat steps 14 to 17 until all the selected voice and call channels are tested.

 **Note:**

If the calls are not cycling through all voice and call channels, then stop the tested voice and call channels. This forces the next call to go to the untested voice and call channels. When you stop the channels, there may be a short delay before the channels go to Off Duty state. This is because stopped channels go into a 1-minute standby mode so they are ready for the next call.

19. Stop the voice and call channels that were tested.
20. Repeat steps 5 to 19 until all voice channels and the same number of call channels are tested.

To test call channels and fax channels

 **Note:**

If CallPilot has no fax channels, go to [To test call channels and speech recognition channels](#) on page 144.

1. In CallPilot Manager, click System -> Service Directory Number.
Result: The Service Directory Number page appears.
2. In the Service Directory Number page, click the Voice Messaging Service DN that you have been using for testing.
Result: The SDN Detail page appears showing the properties of the Voice Messaging Service DN.
3. In the Media Type box, select Fax.

 **Note:**

You can leave the Application Name as Voice Messaging.

4. Click Save.
5. Click Maintenance -> Multimedia Monitor.

Result: The Multimedia Monitor appears.

6. In the Multimedia Monitor page, select and start a maximum of eight fax channels for testing.

 **Note:**

Avaya recommends that you test a maximum of eight fax channels at one time. For example, if you have a 96-channel system, start only eight fax channels. When those eight fax channels are tested, stop them and start another set of fax channels.

7. Stop all voice and speech recognition channels, if these channels are present.
8. Verify that all fax channels are in Idle state, and leave the Multimedia Monitor page open so that you can observe when channels change to Active state.
9. In CallPilot Manager, click Maintenance -> Channel Monitor.

Result: The Channel Monitor appears.

10. Select the whole system and stop all channels.
11. Select and start the same number of call channels as fax channels that you started.

Example: If you have started 8 fax channels, then start eight call channels.

 **Note:**

Ensure that you select and start call channels that have not already been tested (for example, as part of the voice channel test).

12. On the CallPilot server desktop, click Start -> Programs -> CallPilot -> System Utilities -> System Monitor.

Result: The CallPilot System Monitor window appears. By default, the Channel Monitor tab appears on top.

13. Observe the System Monitor window and verify that all the required multimedia (DSP) and call channels are in Idle state, and that all other channels are Off Duty (out of service).
14. Use a telephone to dial the service DN that you entered in the SDN table.
15. Verify that CallPilot answers the call and that the CallPilot greeting plays.
16. Observe the System Monitor and record which call channel and which fax channel change to Active states.
17. Hang up the phone.

18. Repeat steps 14 to 17 until all the selected fax and call channels are tested.

 **Note:**

If the calls are not cycling through all fax and call channels, then stop the tested fax and call channels. This forces the next call to go to the untested fax and call channels. When you stop the channels, there may be a short delay before the channels go to Off Duty state. This is because stopped channels go into a 1-minute standby mode so they are ready for the next call.

19. Stop the fax and call channels that were tested.
20. Repeat steps 5 to 19 until all fax channels and the same number of call channels are tested.

To test call channels and speech recognition channels

1. In CallPilot Manager, click System -> Service Directory Number.

Result: The Service Directory Number page appears.

2. In the Service Directory Number page, click the Voice Messaging Service DN that you have been using for testing.

Result: The SDN Detail page appears showing the properties of the Voice Messaging Service DN.

3. In the Media Type box, select Speech Recognition.

 **Note:**

You can leave the Application Name as Voice Messaging.

4. Click Save.
5. Click Maintenance -> Multimedia Monitor.

Result: The Multimedia Monitor appears.

6. In the Multimedia Monitor page, select and start a maximum of eight speech recognition channels for testing.

 **Note:**

Avaya recommends that you test a maximum of eight speech recognition channels at one time. For example, if you have a 96-channel system, start only eight speech recognition channels. When those eight channels are tested, stop them and start another set of speech recognition channels.

7. Stop all fax and voice channels, if these channels are present.
8. Verify that all speech recognition channels are in Idle state, and leave the Multimedia Monitor page open so that you can observe when channels change to Active state.
9. In CallPilot Manager, click Maintenance -> Channel Monitor.

Result: The Channel Monitor appears.

10. Select the whole system and stop all channels.
11. Select and start the same number of call channels as speech recognition channels that you have started.

Example: If you started eight speech recognition channels, then start eight call channels.

 **Note:**

Ensure you select and start call channels that have not already been tested (for example, as part of the voice or fax channel test).

12. On the CallPilot server desktop, click Start -> Programs -> CallPilot -> System Utilities -> System Monitor.

Result: The CallPilot System Monitor window appears. By default, the Channel Monitor tab appears on top.
13. Observe the System Monitor window and verify that all the required multimedia (DSP) and call channels are in Idle state, and that all other channels are Off Duty (out of service).
14. Use a telephone to dial the service DN that you entered in the SDN table.
15. Verify that CallPilot answers the call and that the CallPilot greeting plays.
16. Observe the System Monitor and record which call channel (on the Channel Monitor page) and which speech recognition channel (on the Multimedia Monitor page) change to Active states.
17. Hang up the phone.
18. Repeat steps 14 to 17 until all the selected speech recognition and call channels are tested.

 **Note:**

If the calls are not cycling through all speech recognition and call channels, then stop the tested speech recognition and call channels. This forces the next call to go to the untested speech recognition and call channels. When you stop the channels, there may be a short delay before the channels go to Off Duty state. This is because stopped channels go into a 1-minute standby mode so they are ready for the next call.

19. Stop the speech recognition and call channels that were tested.
20. Repeat steps 5 to 19 until all speech recognition channels and the same number of call channels are tested.

To restore the SDN Table and put all channels back in service

1. In CallPilot Manager, click System -> Service Directory Number.

Result: The Service Directory Number page appears.
2. In the Service Directory Number page, select the check box for the Voice Messaging Service DN that you have been using for testing.

3. Click Delete Selected.

Result: The Service DN is deleted.



If you are ready to begin CallPilot administration, you can choose to keep this Service DN. However, ensure that the Service DN is configured as required for normal operation. For example, do not leave the Service DN set to the ACD DN.

4. In CallPilot Manager, click Maintenance / Channel Monitor.

Result: The Channel Monitor appears.

5. In the Channel Monitor page, select the whole system and start all channels.

6. Verify that all call channels are in Idle state.

7. Click Maintenance / Multimedia Monitor.

Result: The Multimedia Monitor appears.

8. In the Multimedia Monitor page, select the whole system and start all channels.

9. Verify that all multimedia channels are in Idle state.

Result: The CallPilot tests are completed.

What is next?

Once your testing indicates that the server upgrade, new installation, configuration, platform migration, or system rebuild is successful, perform a full system backup. See "Backing up and restoring CallPilot information," in the *CallPilot Administrator's Guide*(NN44200-601) for more information.

Chapter 7: Avaya CallPilot® 5.0 ELAN IPsec

This chapter describes the configuration procedures for providing communication security between the Avaya CallPilot server and the Communication Server 1000 (CS 1000) on the Embedded LAN (ELAN). IPsec secures the ELAN Application Module Link (AML) connection.

Overview

The Microsoft IP Security (IPsec) protocol protects data traffic running on IP networks by preventing certain known types of attacks. Microsoft IPsec for CallPilot ELAN connections prevents potential security violations. You configure and assign CallPilot ELAN IPsec policy through the Windows 2003 MMC console. The ELAN IPsec policy does not affect normal CallPilot operations, and does not require CallPilot software changes.

 **Note:**

When you configure and assign IPsec to the CallPilot server, you must also configure and assign IPsec to the CS 1000 that shares the same ELAN subnet. For information about configuring IPsec on the CS 1000, see the document *Security Management Fundamentals* (NN43001-604). You must work closely with the CS 1000 administrator when configuring and assigning ELAN IPsec.

The IPsec feature requires minimal administration after you set it up. You can monitor security events in the Event Viewer. When the CS 1000 security parameters are updated, the CallPilot ELAN IPsec policy must be updated accordingly. When you change the ELAN IPsec parameters, you must unassign the ELAN IPsec policy, reconfigure the policy, and assign the policy back to the CallPilot server.

ELAN IPsec requirements

CallPilot ELAN IPsec is supported on the following platforms running CallPilot 5.0 and later:

- 703t
- 600r
- 1005r

CallPilot ELAN IPsec is supported on the CS 1000 running Release 5.0 and later.

IPsec is not supported on a CallPilot High Availability system or on CallPilot with Contact Center integration.

Full mode IPsec is not supported on CallPilot.

Information required for configuring IPsec

Before you configure the ELAN IPsec policy, you must obtain the following information:

- The preshared key (obtained from the CS 1000 administrator)
- The CallPilot ELAN subnet address and subnet mask
- The CS 1000 ELAN subnet address and subnet mask

IPsec configuration overview

For the new CallPilot installation, assign the ELAN IPsec policy to CallPilot before you run the CallPilot Setup Wizard and Configuration Wizard (ConfigWizard). If IPsec is not configured and assigned to the CS 1000 when the CallPilot server is brought into service, the ELAN subnet does not establish connectivity and CallPilot cannot accept calls.

Use the following procedure to configure and assign ELAN IPsec on a new CallPilot server.

Configuring IPsec on a new CallPilot server

At the administrator's PC,

1. Power the CallPilot server on.
The CallPilot server runs a mini-setup procedure during which it performs several reboots before the administrator logon window appears.
2. Log on as the administrator.
Do not run the CallPilot Setup wizard.
3. Configure the IPsec policy on this server. See [Configuring IPsec on your CallPilot server](#) on page 149.
4. Run the CallPilot Setup wizard and Configuration wizard, and configure your CallPilot server.
5. When the CallPilot server powers up, log on to the Administrator account.
6. Open a DOS command window, and check the ELAN IP connection to the Call Server by executing the command: ping <CS ELAN IP address>.

7. If the ELAN connection fails, see [Troubleshooting](#) on page 158 to resolve the problem.
8. If the ELAN connection is successful, the CallPilot services start automatically. CallPilot comes into full service in a few minutes.

The IPsec configuration procedures for an existing CallPilot server are different from those of the first scenario. CallPilot software configurations are previously installed.

Configuring IPsec on an existing CallPilot server

Important:

To minimize the downtime, coordinate this activity with the CS 1000 administrator.

At the administrator's PC,

1. Log on to the CallPilot server as the administrator.
Ignore all the CallPilot error windows and messages.
2. Configure the ELAN IPsec policy on this server. See [Configuring IPsec on your CallPilot server](#) on page 149.
3. After the CallPilot restarts, log on as the administrator.
4. Open a DOS command window and check the ELAN IP connection to the Call Server by executing the command: ping <CS ELAN IP address>.
5. If the ELAN connection is successful, the CallPilot services start automatically. CallPilot comes into full service in a few minutes.
6. If the ELAN connection fails, see [Troubleshooting](#) on page 158 to resolve the problem.

Configuring IPsec on your CallPilot server

These sections provide steps for creating a custom IPsec MMC console and the IPsec policy.

Creating a custom IPsec MMC console

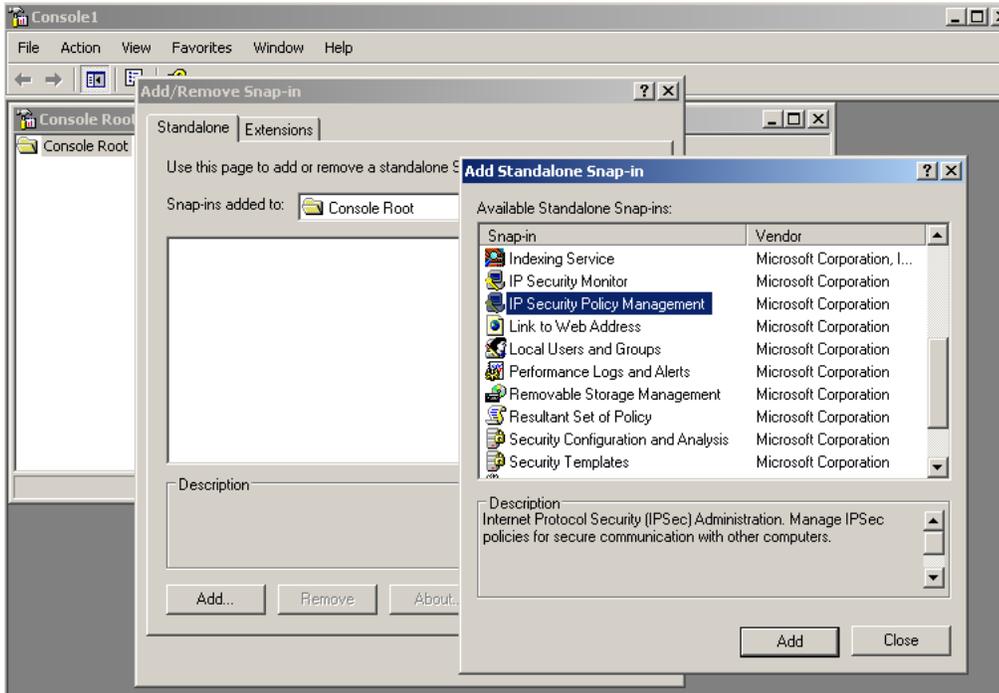
This section describes the steps to configure the MMC console plug-in for IPsec.

Configuring the MMC console plug-in for IPsec

From the CallPilot server,

1. Log on to the CallPilot server as the administrator.
2. From the Windows Start menu, click Run.
3. In the Open text box type mmc.

4. Click OK.
5. In the Console menu, click File and Add/Remove Snap-in.
6. In the Add/Remove Snap-in dialog box, click Add.



7. In the Add Standalone Snap-in dialog box, click IP Security Policy Management, and then click Add.
8. Verify that Local Computer is selected, and click Finish.
9. To close the Add Standalone Snap-in dialog box, click Close.
10. To close the Add/Remove Snap-in dialog box, click OK.
11. In the Console menu, click File and Save As.
12. In the File name box, type IPsec MMC console and click Save.

Creating and configuring IPsec policy

Use the following procedures to create and configure the CallPilot IPsec policy.

Creating the IPsec policy

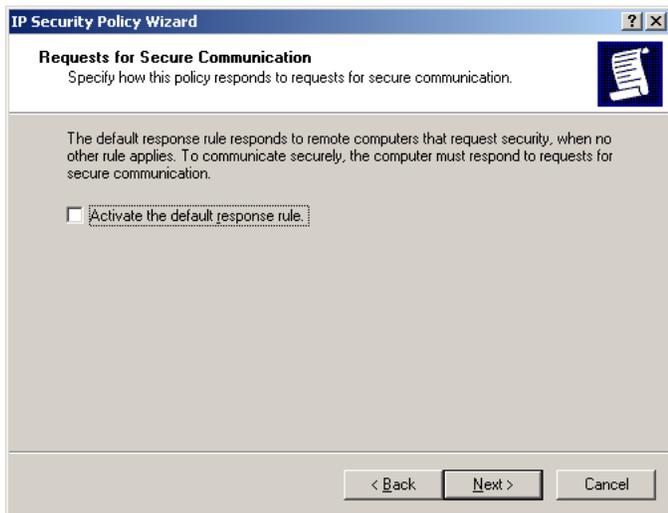
From the Windows desktop,

1. Click Start > Programs > Administrative Tools > IPsec MMC console.msc.
2. On the left pane, select IP Security Policies and right-click IP Security Policies on Local Computer Policy.

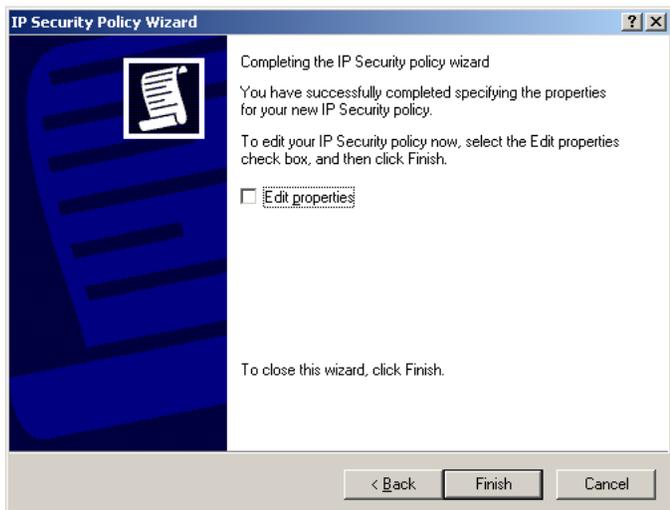
3. Click Create IP Security Policy.
The IP Security Policy Wizard starts.
4. Click Next to continue.



5. In the Name box, type CallPilot ELAN IPsec Policy.
6. In the Description box, type a description and then click Next.



7. Clear the Activate the default response rule check box and click Next.

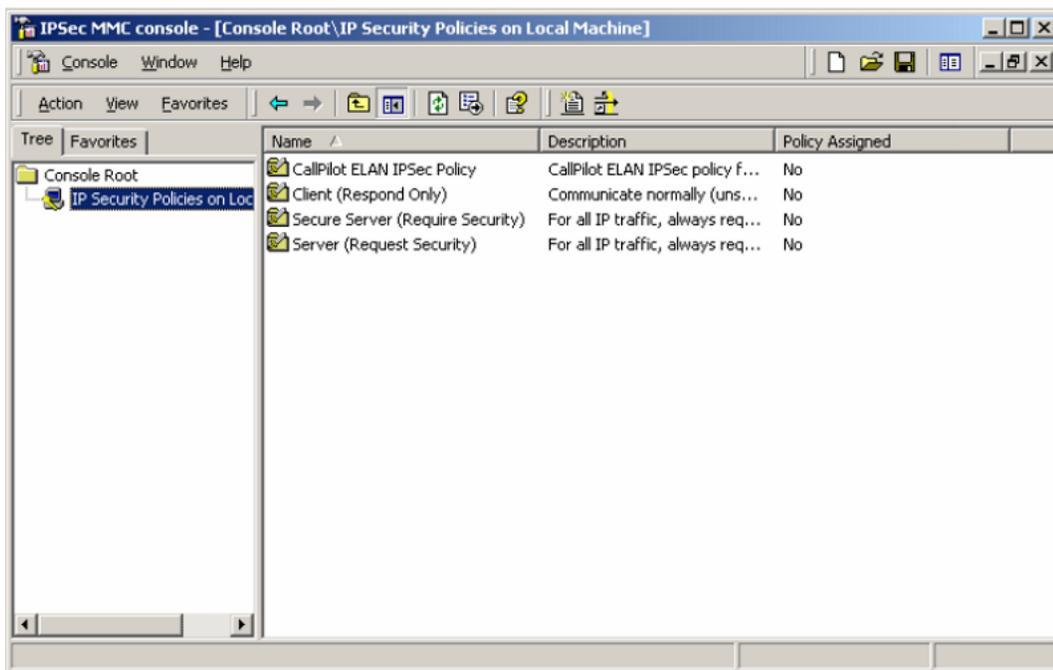


8. Clear the Edit properties check box and click Finish.

9. Go back to the IPsec MMC console.

On the right pane of the console, a new row named CallPilot ELAN IPsec Policy is created. This new policy is not yet configured.

10. Click File > Save.



Configuring the CallPilot ELAN IPsec Policy

From the Windows desktop,

1. Click Start > Programs > Administrative Tools > IPsec MMC console.msc.
2. In the right pane of the IPsec MMC console, right-click CallPilot ELAN IPsec Policy and click Properties.

The CallPilot ELAN IPsec Policy Properties dialog box appears.

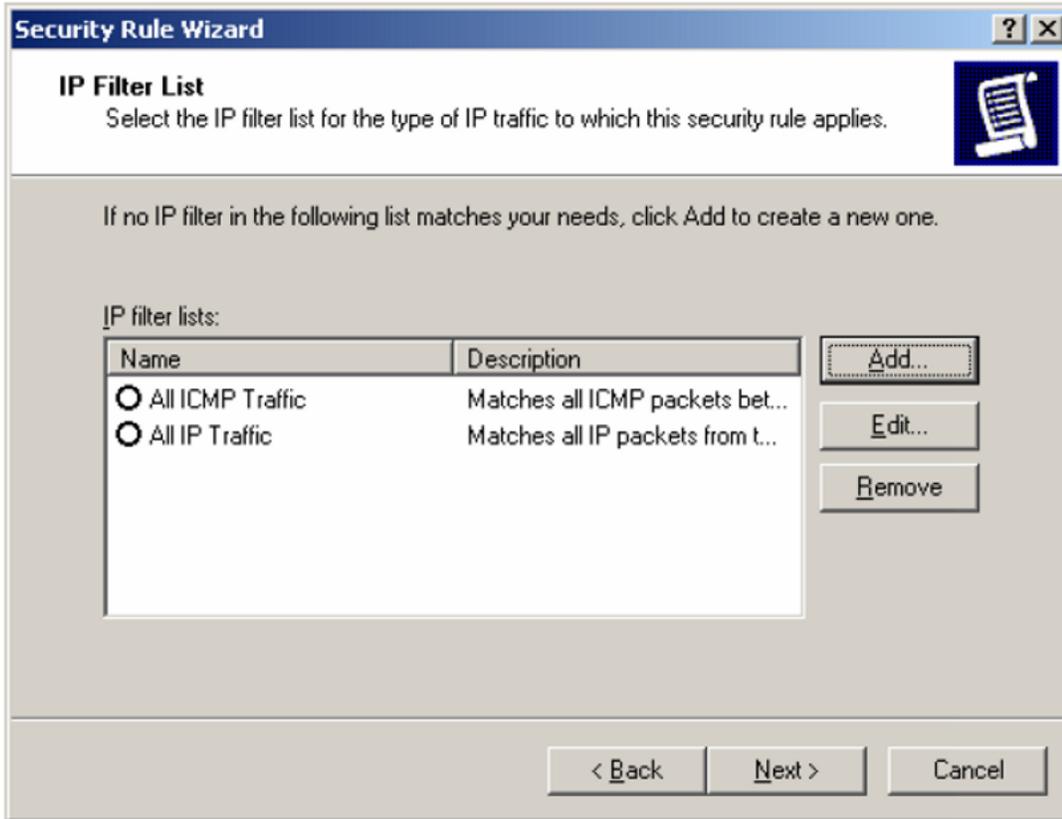
3. In the properties dialog box, select the Rules tab and click Add.

The Security Rules Wizard appears.

4. Click Next.
5. In the Tunnel Endpoint section, select the This rule does not specify a tunnel check box and click Next.
6. In the Network Type section, select the All network connections check box and click Next.
7. In the Authentication Methods section, select the Use this string to protect the key exchange (preshared key) check box.
8. In the text box, type the preshared key string.

The key string is the Security Association transport mode preshared key used in the CS IPsec policy configuration. The key string must be obtained from the CS administrator.

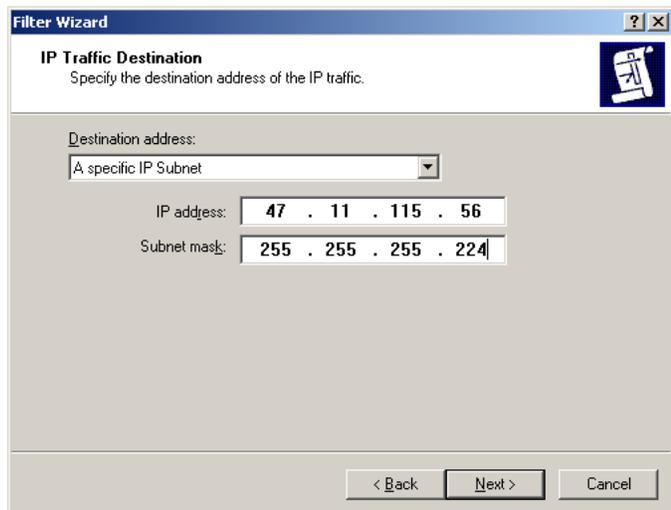
9. Click Next.
10. In the IP Filter List section, click Add. The IP filter list dialog box appears.



11. In the Name box, type All ELAN IP Traffic.
12. In the Description text box, type your description.
13. In the IP Filter List dialog box, click Add.
The IP Filter wizard dialog box appears.
14. Click Next.
15. In the IP traffic source section, select My IP Address from the list.
16. Click Next.

 **Note:**

If you rerun the CallPilot ConfigWizard to modify the CallPilot ELAN IP address, you must reconfigure the CallPilot ELAN IP filter properties in the CallPilot ELAN IPsec Policy.



17. In the IP traffic destination section, select A specific IP subnet from the list.
18. Type the ELAN subnet IP address and the subnet mask and click Next.
19. In the IP protocol type section, select Any from the list.
20. Click Next.
21. Click Finish.
22. Click Close to close the IP Filter List dialog box.
23. In the Security Rule Wizard dialog box, select the newly created filter list All ELAN IP traffic.
24. Click Next.
25. In the Filter Action dialog box, click Add.
The Filter Action Wizard appears.
26. Click Next.
27. In the Filter Action Name section, in the Name box, type ELAN Security.
28. In the Description box, type your description.
29. Click Next.
30. In the Filter Action General Options, select the Negotiate security check box and click Next.
31. In the Communicating with computers that do not support IPSec section, select Do not communicate with computers that do not support IPSec and click Next.
32. In the IP Traffic Security section, select Integrity and Encryption .
33. Click Next.
34. Click Finish.
35. In the Security Rule Wizard dialog box, select the newly created filter action ELAN Security click Edit.

The ELAN Security Properties dialog box appears.

36. Select the Security Methods tab.
37. Select the Use session key Perfect Forward Secrecy check box.
38. Click OK.
39. In the Security Rule Wizard dialog box, select the newly created filter action ELAN Security check box.
40. Click Next > Finish.
41. In the CallPilot ELAN IPsec Policy Properties dialog box, select the ALL ELAN IP Traffic check box.
42. To close the CallPilot ELAN IPsec Policy Properties dialog box, click File > Save > Close.

Starting the Windows IPsec Services

For Windows 2003 to work in IPsec mode, a service called IPsec Services must start. This service does not start by default. Use the following steps to start this service and configure it as an automatic start.

Starting IPsec Services and configuring it to automatically start

From the Windows desktop,

1. Click Start > Programs > Administrative Tools > Services.
2. On the right pane, select IPsec Services, right-click and select Properties.
3. Choose the startup type Automatic (Windows 2003 will start this service automatically when the service is not running).
4. Click Start and then click OK.

Assigning ELAN IPsec Policy to your CallPilot server

Assigning the CallPilot ELAN IPsec Policy to the CallPilot server must be synchronized to enable CS 1000 IPsec mode, if the CS 1000 is already running and is working in IPsec mode. If the CS 1000 is not running in IPsec mode, see the Avaya document CS 1000 OAM Security Feature Specification for information about how to enable CS 1000 IPsec mode.

Use the following steps to assign the CallPilot ELAN IPsec Policy to the local CallPilot server.

Assigning CallPilot ELAN IPsec Policy

From the Windows desktop,

1. Click Start > Programs > Administrative Tools > IPsec MMC console.msc.
2. On the left pane of the console, click the Tree tab and select IP Security Policies on Local Machine.
3. On the right pane, right-click the CallPilot ELAN IPsec Policy and click Assign.
The Policy Assigned column displays Assigned.
4. If the Policy Assigned column shows Assigned, but the IPsec Policy Agent Service shows Assigned, but the IPsec Policy agent service is not in a running state message, see the troubleshooting steps at the end of this chapter.
5. Open a DOS command window. Check the ELAN IP connection to the Call Server by executing the command: ping <CS ELAN IP address>.
6. If the ping returns the message Request timed out., the ping is not successful and the CS 1000 is not reachable. See the troubleshooting section at the end of this chapter.
7. If the ping returns the message Negotiating IP Security each time you run the ping command, the ping is partially successful. The ELAN connection is not working in IPsec mode yet. See the troubleshooting section at the end of this chapter.
8. If the ping returns the message Negotiating IP Security first and then the message Reply from, the ping is successful. The ELAN connection is working in IPsec mode.

Unassigning the CallPilot ELAN IPsec Policy

When you change IPsec parameters on the CS 1000 or the CallPilot ELAN IP address, you must reconfigure the CallPilot ELAN IPsec policy to reflect these changes. You must temporarily disable the CallPilot IPsec mode by unassigning the CallPilot ELAN IPsec Policy.

Unassigning the IPsec Policy

 **Important:**

Coordinate this procedure with the CS 1000 administrator for minimum system downtime.

1. From the Windows desktop, click Start > Programs > Administrative Tools > IPsec MMC Console.msc .
2. In the left pane of the Console window, expand the tree.
3. Select IP Security Policies on Local Computer.
4. In the right pane of the Console window, right-click CallPilot ELAN IPsec Policy.
5. Click Un-assign.

Troubleshooting

To troubleshoot IPsec policy configuration and Internet Key Exchange (IKE) negotiation, you must understand the IKE and IPsec protocols. This section discusses some of the most commonly encountered IPsec problems, which are often caused by a parameter mismatch in the CallPilot ELAN IPsec policy configuration.

To resolve these IPsec configuration issues often requires the cooperation of the CS 1000 administrator.

Problem: After assigning the IPsec policy to the CallPilot server, the following error message appears: Assigned, but the IPsec Policy Agent Service is not in a running state.

Solution: This issue occurs when Windows 2003 IPsec Services are not started. See [Starting the Windows IPsec Services](#) on page 156 for information about starting the Windows 2003 IPsec Services.

Problem: The Ping CS 1000 command returns Request timed out.

Solution: This issue occurs when the CS 1000 is not reachable. The CS 1000 is not powered up or the IP path to CS 1000 fails (gateway routers, hubs, and cables). Unassign the CallPilot ELAN IPsec Policy, and check the IP path to CS using utility tools like ping.exe and tracert.exe.

Problem: Ping CS 1000 always returns Negotiating IP Security.

Solution: This problem occurs when IPsec IKE negotiation passes phase 1 but fails at phase 2. The CS 1000 is reachable on the ELAN subnet, but parameter mismatches occur in the CallPilot ELAN IPsec Policy. Print the policy parameters and check with the CS 1000 administrator for mismatches. For printing instructions, see [Printing IPsec policy parameters](#) on page 158. When you identify the mismatched parameters, reconfigure the parameters.

Printing IPsec policy parameters

If your troubleshooting procedures indicate a parameter mismatch, you can print the policy information to a file. To print the policy information, use the Netsh.exe command. The format of the command follows:

```
C:\>netsh IPsec static show policy <"policy name"> level = verbose > <filename>
```

The following is an example of a request to print the policy information to a file named CP_ELAN_IPsec_Policy_summary.txt:

```
netsh IPsec static show policy "CallPilot ELAN IPsec Policy" level=verbose >
CP_ELAN_IPsec_Policy_summary.txt
```



In the following examples, the parameters in bold are most likely to cause problems if they are mismatched.

Avaya CallPilot® 5.0 ELAN IPsec

```
Policy Name           : CallPilot ELAN IPsec Policy
Description           : NONE
Store                 : Local Store <CPLAB231B>
Last Modified        : 2/8/2007 8:25:59 PM
GUID                  : {6E5972CC-F7EF-416B-A53E-FDE7CB02CED4}
Assigned              : NO
Polling Interval     : 180 minutes
MainMode LifeTime    : 480 minutes / 0 Quick Mode sessions
Master PFS           : NO
Main Mode Security Method Order
  Encryption          Integrity          DH Group
  -----
  3DES                SHA1                Medium(2)
  3DES                MD5                 Medium(2)
  DES                 SHA1                Low(1)
  DES                 MD5                 Low(1)

No. of Rules         : 2

Rule Details
-----

Rule ID              : 1, GUID = {36492C90-7528-4D32-A728-D0B8FEB7B380}
Rule Name            : NONE
Description          : NONE
Last Modified       : 2/8/2007 8:25:59 PM
Activated           : YES
Connection Type     : ALL
Authentication Methods(1)

    Preshared Key : abc123456

FilterList Details
-----

FilterList Name     : All ELAN IP Traffic
Description         : Allow all ELAN IP traffic
Store               : Local Store <CPLAB231B>
Last Modified      : 2/8/2007 8:17:07 PM
GUID                : {3128DD0D-2EAD-4735-A72F-2288D50B7E67}
No. of Filters     : 1
Filter(s)
-----
Description        : NONE
Mirrored           : YES
Source IP Address  : <My IP Address>
Source Mask        : 255.255.255.255
Source DNS Name    : <My IP Address>
Destination IP Address : 47.11.255.0
Destination Mask   : 255.255.255.0
Destination DNS Name : <A Specific IP Subnet>
Protocol           : ANY
Source Port        : ANY
Destination Port   : ANY
```

Figure 33: CallPilot ELAN IPsec Policy file

```

FilterAction Name      : ELAN Security
Description            : NONE
Store                 : Local Store <CPLAB231B>
Action                : NEGOTIATE SECURITY
AllowUnsecure(Fallback) : NO
Inbound Passthrough   : YES
QMPFS                 : YES
Last Modified         : 2/8/2007 8:23:28 PM
GUID                  : {581E241B-DD1F-4E34-8767-9843901EE580}

```

```

Security Methods
  AH      ESP      Seconds      kBytes
  ---      ---      -
[NONE]    [SHA1 , 3DES]      0      0

```

```

Rule ID                : 2, GUID = {EC6E0009-C88B-42F4-89C3-07C44DFAA48E}
Rule Name              : NONE
Description            : NONE
Last Modified         : 2/8/2007 8:08:35 PM
Activated              : NO
Connection Type       : ALL
Authentication Methods(1)

```

KERBEROS

No FilterList exists in Default Response Rule

FilterAction Details

```

-----
FilterAction Name      : NONE
Description            : NONE
Store                 : Local Store <CPLAB231B>
AllowUnsecure(Fallback) : NO
Inbound Passthrough   : NO
QMPFS                 : NO
Last Modified         : 2/8/2007 8:08:35 PM
GUID                  : {1B122FF1-A4B2-4FE2-8E65-B95FC418F4F7}

```

```

Security Methods
  AH      ESP      Seconds      kBytes
  ---      ---      -
[NONE]    [SHA1 , 3DES]      0      0
[NONE]    [MD5 , 3DES]      0      0
[NONE]    [SHA1 , DES ]      0      0
[NONE]    [MD5 , DES ]      0      0
[SHA1]    [NONE , NONE]      0      0
[MD5 ]    [NONE , NONE]      0      0

```


Index

C

customer service [9](#)

D

distributor [9](#)

documentation [9](#), [12](#)

 map [12](#)

R

reseller [9](#)

T

training [9](#)

